**UNIVERSIDADE FEDERAL DE SANTA CATARINA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO**

Emily Vivian Valcarenghi

# IMPACTOS DA ADOÇÃO DA CERTIFICAÇÃO DIGITAL ICP-BRASIL

Dissertação submetida ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina para a obtenção do Grau de Mestre em Engenharia do Conhecimento.
Orientador: Prof. João Artur de Souza, Dr.
Coorientador: Profª Gertrudes Aparecida Dandolini, Drª

Florianópolis
2015

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Valcarenghi, Emily Vivian
Impactos da adoção da certificação digital ICP-Brasil / Emily Vivian Valcarenghi ; orientador, João Artur de Souza ; coorientadora, Gertrudes Aparecida Dandolini. - Florianópolis, SC, 2015.
216 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento.

Inclui referências

1. Engenharia e Gestão do Conhecimento. 2. Certificação Digital. 3. Impacto. 4. Adoção. 5. Segurança do Conhecimento. I. de Souza, João Artur. II. Aparecida Dandolini, Gertrudes. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. IV. Título.

**EMILY VIVIAN VALCARENGHI**

**IMPACTOS DA ADOÇÃO DA CERTIFICAÇÃO DIGITAL ICP-BRASIL**

Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Engenharia e Gestão do Conhecimento, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina.

Florianópolis, 19 de março de 2015.

_____
Prof. Roberto Carlos dos Santos Pacheco, Dr.
Coordenador do Curso

**Banca Examinadora:**

_____
Prof. João Artur de Souza, Dr.
Orientador

_____
Prof. Aires José Rover, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Édis Mafra Lapolli, Drª.
Universidade Federal de Santa Catarina

_____
Prof. Ricardo Azambuja Silveira, Dr.
Membro Externo

Dedico esta conquista à minha família, em especial aos meus pais, René e Terezinha, que sempre foram meu esteio e exemplo, à minha irmã Rafaela, pelo apoio, carinho, paciência e incentivo recebidos em todos os momentos desta caminhada. E a meus orientadores Prof. Dr. João Artur e Profª. Drª Gertrudes, pelo carinho, paciência e orientação.

## AGRADECIMENTOS

O desenvolvimento desta dissertação não seria possível sem a participação direta ou indireta de algumas pessoas, às quais gostaria de agradecer neste espaço.

Primeiramente aos meus pais, René e Terezinha, pessoas a quem devo eterna gratidão, pois além de muito amor, carinho e educação, sempre estiveram ao meu lado possibilitando a minha dedicação aos estudos e dando condições para o meu desenvolvimento pessoal, profissional e acadêmico. Vocês são meu exemplo e os amo mais do que tudo.

A minha irmã e melhor amiga Rafaela Vivian Valcarenghi, obrigada por me acalmar e compreender e tentar sempre que possível contribuir com esta pesquisa, obrigada por ser este exemplo de coração gigante e delicado que você é. Você sempre foi e sempre será o meu anjo e o meu orgulho, te amo.

À minha "filhotinha" e companheira Sophie, que muitas vezes subia no computador para pedir atenção e mais tarde me dar o dobro de atenção e carinho. Não somos nada sem o amor de nossos anjos peludos.

A meus irmãos René Júnior, Flávia, Aluísio, Luciano, Pietro e Rafaela, meus sobrinhos Franciere, Gabriel e Fábio, as minhas cunhadas e cunhados, obrigada por fazerem parte da minha vida.

Aos demais membros da família, que torcem pelo sucesso de todos.

Ao meu noivo, Jobson Oliveira, que aos poucos vem me cativando e conquistando. Obrigada pelo carinho.

Apesar de não ter algo muito sólido, agradeço a Deus e ao Plano espiritual, que principalmente nas horas de aperto, me agarro.

Às minhas melhores amigas e grandes mulheres Carolina Fabrícia Narciso, Graziele Bonini, Lisiane Marques, Luciane Adolfo, Marcela Rosa, Thiana Sebben Pasa, pelo carinho e exemplo que há anos vem me trazendo para a realidade, minhas irmãs de coração.

Aos meus amigos de Caçapava do Sul, em especial Dayane Madrid, Karen Veber, Kellen Veber, Jaqueline Fagundes, Tairise Valcarenghi, Rossi Lopes, Jorge Cruz, Lenon Mello, William Lopes, que ajudaram diversas vezes a aliviar a tensão... bora fazer um churrasco para comemorar.

À minha família do Hospital Universitário, em especial à Jaciete Maria Pinto Felipe, Irma do Carmo de Souza Pereira e Nilzete Vieira (minhas três mãezinhas do coração). Ainda à Norivaldo Vieira, Célio

Coelho, Sandra Regina Costa, Drª Eliane Matos, Profª Maria Rovaris, Drª Heda Mara Schmidt, Profª Raquel Kuerten de Salles, Prof. Paraná, Nélio Schmitt, Paulo Portella, Allan Duwe, Mara Sérgia Pacheco, Nicéia Mara Almeida, Profª Francine Lima Gelbcke, Prof. Felipe Felício, Jussemara Matta, Juliana Santos e estagiárias: Raynara Esmeraldino, Rayana Arceno, Kelly Steinert, Brunna Tolentino, Júlia Melo, Karen Laíse Moroski, Camila Francisco e demais que por lá já passaram. Ao Cleiton Nascimento, pela camaradagem e simpatia de sempre.

Aos amigos de Florianópolis Paulo Bueno e Fernando Augusto Fonseca que sempre me incentivaram a entrar no mestrado e por serem profissionais e pessoas que admiro muito.

Às meninas do apto 203, Roberta Tono e Maria Laura Monteiro, que entendem sempre o meu isolamento.

Aos Professores João Artur de Souza e Gertrudes Aparecida Dandolini, por terem me aceitado no Programa de Pós-graduação de Engenharia e Gestão do Conhecimento e pelo empenho e paciência em orientar-me. Ambos sempre com muito carinho e atenção, dando à todos os alunos do grupo de pesquisa IGTI - Núcleo de Estudos em Inovação, Gestão e Tecnologia da Informação– e à seus orientandos não só orientação, mas criando um ambiente familiar e amigável de união, companheirismo e trabalho em grupo.

Aos demais professores e colegas do IGTI em especial aos colegas Roberto Fabiano Fernandes, Michele Andrea Borges, Pierry Teza e Maurílio T. B. Schmitt, que sempre me auxiliaram com suas experiências e conhecimentos.

Aos professores do Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento que aceitaram compor a banca examinadora. É uma grande honra tê-los como avaliadores desta pesquisa.

Ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, pela oportunidade em participar desse prestigiado curso.

Agradeço também a todas as pessoas que participaram direta ou indiretamente do desenvolvimento desta pesquisa.

**Muito obrigada!**

“Todos os homens por natureza desejam conhecer”. (Aristóteles)

## RESUMO

VALCARENGHI, Emily Vivian. **Impactos da adoção da certificação digital ICP-Brasil**, 2014. Mestrado em Engenharia e Gestão do Conhecimento – Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, UFSC, Florianópolis, Brasil.

Com a explosão do uso da internet para os mais variados fins, gerando um ambiente repleto de possibilidades e também de incertezas, há o aparecimento de diversas Tecnologias de Informação e Comunicação e uma preocupação com relação a segurança da informação e do conhecimento em transações eletrônicas nas organizações. Neste contexto, surge no Brasil, em 2001 a Infraestrutura de Chaves Públicas – ICP-Brasil, mantida pelo Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal, que regulamenta a certificação digital, tecnologia utilizada para garantir autenticidade, confidencialidade e a integridade de informações, conferindo-lhe validade jurídica. O presente estudo teve o objetivo de analisar o impacto percebido por especialistas na adoção da certificação digital ICP-Brasil. Trata-se de uma pesquisa qualitativa, descritiva e exploratória, em que para coleta de dados foram realizadas entrevistas abertas. A técnica de análise de conteúdo foi utilizada, o que permitiu a extração dos dados das entrevistas quanto aos aspectos referentes às potencialidades e fragilidades da certificação digital no Brasil. Utilizou-se a visão sistêmica, através do modelo CESM, para identificar os atores, componentes, ambiente, estrutura e mecanismos, bem como a fronteira. Conclui-se que os benefícios ou potencialidades decorrentes do uso da certificação digital abrangem direta e indiretamente, desde agilidade nos processos, até a economia verde, pela redução do uso do papel; através da desmaterialização dos processos; segurança das informações e acessibilidade, beneficiando relacionamentos interorganizacionais; além de que ter sido verificado que o número de aplicações com uso de certificado digital está crescendo a cada ano e aos poucos vai sendo disseminado na sociedade. Como fragilidades aponta-se o alto custo do certificado; as questões culturais, onde muitos usuários têm receio com novidades; a dificuldade de instalação da cadeia de certificado; a própria estrutura da ICP; a falta de unificação dos sistemas, que dificulta a interoperabilidade. Acredita-se que o estudo traga grandes benefícios para que o ITI possa criar estratégias de

difusão e adoção de certificados digitais que minimizem os impactos negativos da tecnologia (custo do certificado, cultura, dentre outros).

**Palavras-chave**: Impacto. Certificação Digital. Adoção. Segurança do Conhecimento.

## ABSTRACT

VALCARENGHI, Emily Vivian. **Impacts of the adoption of digital certification ICP-Brazil**. 2014. Thesis (Master degree in Engineering and Knowledge Management) – Post-Graduate Program in Engineering and Knowledge Management, UFSC, Florianópolis, Santa Catarina, Brazil.

With the explosion of Internet use for various purposes, creating an environment full of possibilities and also of uncertainties, there is the appearance of several Information and Communication Technologies and a concern about the security of information and knowledge in electronic transactions in organizations. In this context, appears in Brazil, in 2001 the Public Key Infrastructure - ICP-Brazil, maintained by the National Institute of Information Technology (ITI), an independent federal agency that regulates the digital certification technology used to ensure authenticity, confidentiality and integrity information, giving it legal validity. This study aimed to analyze the impact perceived by experts in the adoption of digital certification ICP-Brazil. This is a qualitative, descriptive and exploratory research, where data collection open interviews were conducted. The content analysis technique was used which allowed the extraction of data from the interviews in the matters concerning the strengths and weaknesses of digital certification in Brazil. The systemic view was used by the CESM model to identify the actors, components, environment, structure and mechanisms, as well as the border. It is concluded that the benefits or capabilities from the digital certification use cover directly and indirectly, from process agility until the green economy by reducing the use of paper; through dematerialisation of processes; information security and accessibility, benefiting inter-relationships; plus it has been verified that the number of applications with digital certificate use is growing every year and is slowly being disseminated in society. How weaknesses points to the high cost of the certificate; cultural issues, where many users are afraid to news; the difficulty of installation certificate chain; the ICP structure itself; the lack of unification of the systems, which impedes interoperability. It is believed that the study bring great benefits to the ITI can create dissemination strategies and adoption of digital certificates that minimize the negative impacts of technology (cost of the certificate, culture, among others).

**Keywords**: Impact,DigitalCertification,Adoption, knowledge security.

# LISTA DE FIGURAS

# LISTA DE QUADROS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

ABNT NBR ICO/IEC
AC – Autoridade Certificadora
AR – Autoridade de Registro
BTD – Banco de Teses e Dissertações
CAPES –Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CC – Casa Civil
CD – Certificação Digital
CEF – Caixa Econômica Federal
CEGE – Comitê Executivo de Governo Eletrônico
CESM – *Composition-Environment-Structure-Mechanism*
CGSI – Comitê Gestor de Segurança da Informação
CMPR – Casa Militar da Presidência da República
COMPRASNET – Portal de Compras do Governo Federal
CTSR – Câmara Técnica de Serviços de Rede
DAFN – Diretoria de Auditoria, Fiscalização e Normalização
DENATRAN – Departamento Nacional de Trânsito
DINFRA – Diretoria de Infraestrutura de Chaves Públicas
e-CAC – Central Virtual de Atendimento ao Contribuinte
e-PING –Padrões de Interoperabilidade em Governo Eletrônico
EC – Engenharia do Conhecimento
EGC – Engenharia e Gestão do Conhecimento
FEBRABAN - Federação Brasileira de Bancos
FGTS –Fundo de Garantia do Tempo de Serviço
G2B - *Government to Business*
G2C - *Government to Citizen*
G2G –*GovernmenttoGovernment*
GRRF – Guia de Recolhimento Rescisório do FGTS
GSI – Gabinete de Segurança Institucional
GT3 – Grupo de Trabalho de Segurança da Informação
GTI – Grupo de Trabalho Interministerial
GTTI - Grupo de Trabalho em Tecnologia da Informação
IBICT –Instituto Brasileiro de Informação em Ciência e Tecnologia
ICMS – Imposto sobre Circulação de Mercadorias e Serviços
ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira
ICP-Gov - Infraestrutura de Chave Pública do Poder Executivo
IGTI –Núcleo de Estudos em Inovação, Gestão e Tecnologia de Informação
IPI – Imposto sobre Produtos Industrializados
ITI – Instituto Nacional de Tecnologia da Informação
LEA – Laboratório de Ensaios e Auditoria
MC – Ministério de Comunicações
MCTI – Ministério de Ciência, Tecnologia e Inovação

MD – Ministério de Defesa
MEC – Ministério da Educação
MP – Medida Provisória
MTE – Ministério do Trabalho e Emprego
NF-e – Nota Fiscal Eletrônica
OAB – Ordem dos Advogados do Brasil
P&D – Pesquisa e Desenvolvimento
PFE – Procuradoria Federal Especializada
PKI – *Public Key Infrastructure*
PPEGC - Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento
PROUNI – Programa Universidade para todos
RENAJUD – Restrições Judiciais de Veículos Automotores
RENAVAM – Registro Nacional de Veículos Automotores
RES – Registro Eletrônico de Saúde
SCDP – Sistema de Diárias e Passagens
SEFIP - Sistema Empresa de Recolhimento do FGTS
SIAFI - Sistema Integrado de Administração Financeira do Governo Federal
SIAPE - Sistema Integrado de Administração de Recursos Humanos
SIDOF –Sistema de Geração e Tramitação de Documentos Oficiais
SIORG - Sistema de Informações Organizacionais do Governo Federal
SIPREV – Sistema Integrado de Informações Previdenciárias
SISBACEN – Sistema do Banco Central do Brasil
SPB – Sistema de Pagamentos Brasileiro
SPED – Sistema Público de Escrituração Digital
STF – Supremo Tribunal Federal
TCLE – Termo de Consentimento Livre e Esclarecido
TGS - Teoria Geral dos Sistemas
TI – Tecnologia de Informação
TIC – Tecnologia de Informação e Comunicação
TIE – Tecnologias da Informação Emergentes
TPP- Tecnológicas de Produtos e Processos
UFSC - Universidade Federal de Santa Catarina

**SUMÁRIO**

# 1 INTRODUÇÃO

Em uma sociedade em que a única certeza é a incerteza, onde o conhecimento é a principal fonte de vantagem competitiva, organizações têm de se transformar em criadoras de conhecimento em escala global, pois, quando mercados se transformam, as tecnologias proliferam, os competidores multiplicam-se e os produtos se tornam obsoletos rapidamente (NONAKA E TAKEUCHI, 1997).

Neste sentido, organizações de sucesso são aquelas que criam continuamente novos conhecimentos, disseminando-os amplamente pela organização e incorporando-os em novas tecnologias e produtos, ou seja, são organizações que inovam constantemente (NONAKA E TAKEUCHI, 2008). Assim, surge o que se chama sociedade do conhecimento, que é assinalada pela velocidade das informações, onde pessoas adquirem e disseminam conhecimento fazendo uso das informações como ferramenta de crescimento pessoal (FRANTZ, 2011).

Nesta sociedade do conhecimento, o desafio deixou de ser o de cuidar (sociedade agrária) e trabalhar (sociedade industrial), passando a ser o de *criar* conhecimento e gerar aptidão para aplicá-lo, tendo a *mente* como símbolo desta sociedade, a *pessoa* como instituição representativa e a tecnologia e as competências como fonte de valor (SABBAG, 2007).

Percebe-se, desta forma, que o mundo está em um processo de transformação estrutural multidimensional, que está associado à emergência de um novo paradigma tecnológico, baseado nas Tecnologias de Comunicação e Informação – TIC's, onde a exigência primordial é a segurança no tráfego das informações. Sabe-se que tecnologias são particularmente sensíveis aos efeitos de seu uso social, ou seja, elas tomam forma a partir das necessidades, valores e interesses de seus usuários (CASTELLS e CARDOSO, 2005).

Com o uso da internet para os mais variados fins, vem à tona questões sobre proteção da informação e do conhecimento contra um potencial uso indevido, que conforme Baltzan e Phillips (2012) discutem, são questões de ética e segurança da informação, que vão desde qualquer tipo de informação que empresas recolhem e utilizam, incluindo informações sobre clientes, parceiros e funcionários.

Com o intuito de proteger as informações, é utilizada a criptografia, também conhecida como "escrita escondida", mecanismo de codificação, que de maneira sucinta, funciona como um "embaralhamento" das informações para que fique impossível de serem

identificadas por pessoas não autorizadas. No ambiente digital, quanto mais *bits* a chave possui, ou seja, maior o número de combinações, mais dificilmente ela pode ser decodificada. Existem basicamente duas técnicas criptográficas: a criptografia de chave privada ou simétrica (técnica mais antiga) e a criptografia de chave pública ou assimétrica. Diz-se que a criptografia é simétrica, quando emissor e receptor possuem a mesma chave. Já a criptografia assimétrica, exige duas chaves diferentes: uma pública e outra privada. A chave pública é de conhecimento de todos, enquanto a chave privada é a única capaz de traduzir/decodificar a informação. Por exemplo, uma pessoa utiliza minha chave pública para me enviar uma mensagem e somente acesso a mensagem utilizando minha chave privada.

Considerando que, uma vez que informações "caem" nas redes sociais e que elas se disseminam de forma exponencial e descontrolada, o que pode trazer consequências tanto positivas, quanto negativas, seja para organizações, governos ou indivíduos, isto se torna um dos grandes desafios da sociedade do conhecimento: a segurança de informações e conhecimento nas redes.

A tecnologia que utiliza a criptografia e tem sido utilizada para garantir a segurança das informações, ou seja, garantir a autenticidade, a confiabilidade, a integridade e validade jurídica, é a certificação digital. Esta tecnologia é utilizada em diversos países como Alemanha, França, EUA, Espanha, Brasil, entre outros.

O certificado digital ou identidade digital é um arquivo digital, chancelado digitalmente pela entidade emissora, ou seja, por uma Autoridade Certificadora – AC, que tem como objetivo interligar a chave pública a uma entidade ou indivíduo.

Neste capítulo serão tratados os aspectos referentes ao tema em estudo, destacando o problema de pesquisa, objetivo geral e específicos, justificativa, aderência do tema ao Programa de Pós-Graduação de Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina - PPEGC, delimitação e organização desta pesquisa.

## 1.1 TEMA E PROBLEMA DE PESQUISA

A humanidade tem passado por transformações tão vastas e abruptas, que fazem com que os indivíduos tenham dificuldade de assimilar mudanças geopolíticas, sociais, culturais e tecnológicas que os afetam e que afetam tudo a seu redor. Este ambiente onde a incerteza e a

mudança são constantes e abruptas dá origem a uma nova sociedade, a sociedade do conhecimento (FRANTZ, 2011).

Além do ambiente incerto em que a sociedade vive, outro desafio que surge é a forma de lidar com as mais variadas formas de conhecimento, neste sentido, as TIC's impulsionam a gestão do conhecimento ao melhorar seus processos, ligando bancos de dados à seus usuários, bem como, favorecendo a interatividade entre as pessoas, onde através da internet, o indivíduo passa a ser o principal ativo, sendo as relações sociais, a interação e a cooperação características fundamentais para o desenvolvimento virtual, criando assim diversas redes de interação (FRANTZ, 2011).

O comércio eletrônico, os sensores inteligentes, as imagens digitais, a micro engenharia, as tecnologias de segurança de informação e demais tecnologias têm o potencial de reconstruir processos e tornar obsoletas estratégias já estabelecidas; desta forma, a habilidade de dominar tecnologias emergentes é essencial à sobrevivência das organizações, uma vez que pouquíssimas escaparão completamente do impacto das forças causadas por estas novas tecnologias (DAY, SCHOEMAKER E GUNTHER, 2003).

Nas duas últimas décadas houve uma explosão do uso da internet para os mais diversos fins, que vão desde atividades de entretenimento, comunicação, até a realização de transações bancárias; como sistema de informação global interconectado e em constante evolução, com novas interfaces, permitindo a construção de novas redes e de novos conhecimentos e assumindo uma prática colaborativa, que exige processos, métodos ou até mesmo ferramentas ou tecnologias associadas, que garantam segurança a seus usuários, medidas de segurança, como antivírus e *firewalls*, tornam-se vitais.

É importante conhecer as ameaças, e entender as formas de se defender delas pode ser igualmente essencial (TURBAN, MCLEAN E WETHERBE, 2004).

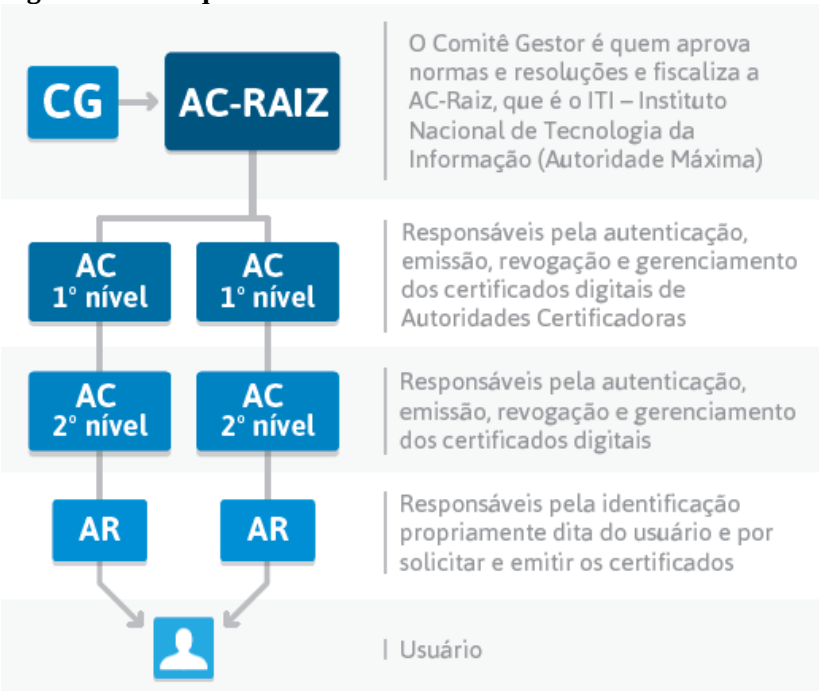
Há uma grande preocupação com segurança, confidencialidade, integridade e autenticidade das informações, uma vez que *antivírus* e *firewalls* não impedem ameaças, como por exemplo, a falsificação ou acesso não autorizado. Neste sentido, países preocupados com a vulnerabilidade das transações eletrônicas têm adotado modelos de infraestrutura de chaves públicas, que garantem transações seguras, através do uso da certificação digital.

No Brasil, a Infraestrutura de Chaves Públicas - ICP-Brasil, acrescenta a validade jurídica e o não repúdio em suas regras de certificação.

Criada em 2001, a ICP-Brasil (Figura 1), tem como objetivo garantir autenticidade, confidencialidade, integridade, não repúdio e validade jurídica às informações eletrônicas, tendo o Instituto Nacional de Tecnologia da Informação - ITI como a Autoridade Certificadora Raiz.

A Figura 1 demonstra a hierarquia da cadeia de confiança da ICP-Brasil, composta por uma Autoridade Certificadora - AC Raiz, que é o ITI, normatizada e fiscalizada por um Comitê Gestor; seguidas das Autoridades Certificadoras – AC's de 1º nível, responsáveis pela certificação das AC's de 2º nível, que por sua vez são responsáveis pelo gerenciamento e emissão dos certificados, que são solicitados e emitidos pelas Autoridades de Registro - AR, que também identificam os usuários dos certificados.

**Figura1: Hierarquia da ICP-Brasil**

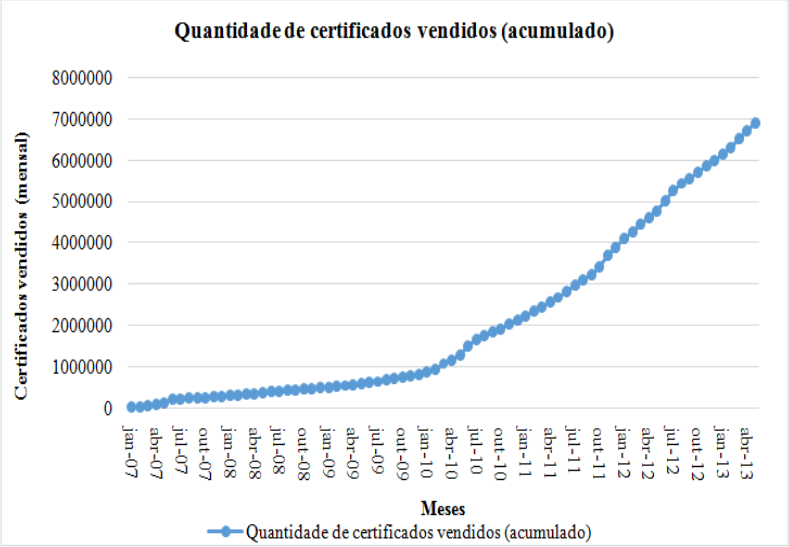



Fonte: Cartilha ICP-Brasil, 2012.

Ao longo dos 14 anos de existência da ICP-Brasil, percebe-se que o crescimento da difusão da certificação digital depende tanto do crescimento da cadeia de confiança (nº de AC's de 1º nível e 2º nível e – AR's) como também do número de aplicativos que utilizam certificação.

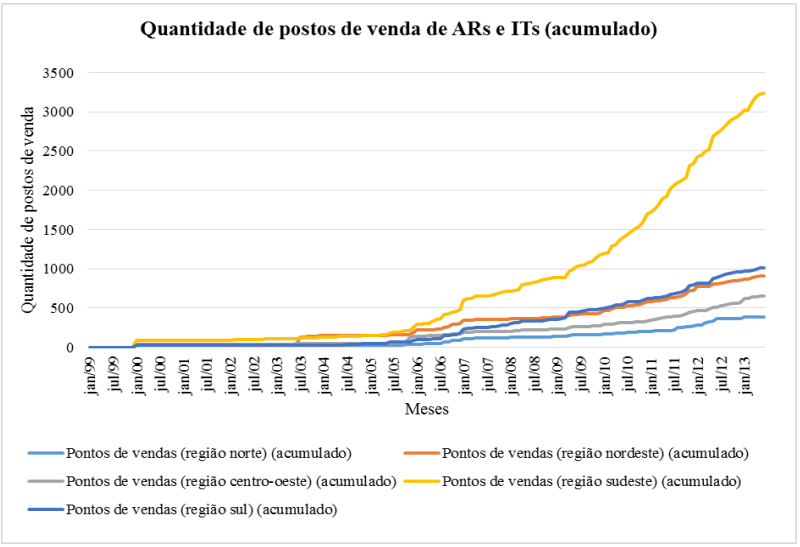
Pode-se acompanhar o aumento do número de certificados vendidos (Figura 2), nos 10 anos de sua implantação no Brasil e a evolução da estrutura de vendas (Figura 3), que demonstram a sua expansão, tornando-se, portanto, importante acompanhar como esta tecnologia tem se comportado e como tem impactado as relações sociais, as relações de trabalho, dentre outras questões.

**Figura 2: Quantidade de certificados vendidos (acumulado)**




Fonte: IGTI (2013)

**Figura 3: Quantidade de postos de venda de ARs e ITs (acumulado)**




Fonte: IGTI (2013)

Os benefícios decorrentes do uso da certificação digital abrangem desde agilidade nos processos, até a economia verde, pela redução do uso do papel. Diversos estudos no Brasil têm buscado entender a certificação digital de modo geral e também, e principalmente sobre algoritmos criptográficos. Porém inexistem trabalhos acadêmicos que tratem da evolução, dos cenários da certificação digital no Brasil (MARTINI, 2008), bem como impactos causados na sua adoção e que apontem o caminho que esta tecnologia está tomando.

Diante do exposto, esta pesquisa propõe-se a analisar o impacto da certificação digital no Brasil, a fim de responder a seguinte pergunta de pesquisa:

**Qual a percepção de especialistas sobre a adoção da certificação digital ICP-Brasil?**

## 1.2 OBJETIVOS

Com base na pergunta de pesquisa, estabeleceram-se os objetivos geral e específicos.

### 1.2.1 Objetivo geral

Analisar o impacto percebido por especialistas na adoção da certificação digital ICP-Brasil.

### 1.2.2 Objetivos específicos

- Realizar um mapeamento da situação atual da certificação digital ICP-Brasil;
- Identificar e definir as dimensões de análise de impacto de tecnologias;
- Caracterizar a certificação digital ICP-Brasil sob uma visão sistêmica;
- Analisar a percepção de especialistas sobre a adoção da certificação digital ICP-Brasil.

## 1.3 JUSTIFICATIVA

Na sociedade do conhecimento, descrita como a combinação das configurações e aplicações da informação com as tecnologias da comunicação em todas as suas possibilidades (SQUIRRA, 2005), no qual conhecimento e informação são compartilhados nas redes sociais em tempo real, surgem novas preocupações: como instigar compartilhamento de conhecimento, mantendo sua segurança, seja de acesso não autorizado, fraudes ou outras questões (ARAUJO, 2009)? Neste sentido, surgem as TIC's, que são uma das principais estratégias de negócios que impactam direta e/ou indiretamente a vida das pessoas. Todavia, elas inovam tão rapidamente, trazendo novas ferramentas, técnicas, práticas e ainda novas necessidades, provocando maiores incertezas.

O crescimento acelerado das incertezas e das mudanças de paradigmas caracterizam o novo século (MORITZ; MORITZ; PEREIRA, 2012), ou seja, as mudanças sociais, econômicas, ambientais, culturais e tecnológicas têm impactado profundamente umas às outras, principalmente nos quesitos inovação e competitividade.

Em meio a tantas mudanças influenciadas cada vez mais pelos avanços tecnológicos e o surgimento de uma nova sociedade marcada pela informação e o conhecimento, torna-se necessário analisar a influência e os pontos positivos e negativos de todo esse processo de inovação tecnológica e informacional na sociedade, contabilizando os impactos de todo esse processo de inclusão digital da população brasileira e a questão da diminuição da exclusão social e pobreza. (TAVARAYAMA, SILVA e MARTINS, 2012)

Portanto, é necessário pensar e planejar à longo prazo, a fim de acompanhar o progresso tecnológico, sua difusão e adoção, bem como a análise de qual o caminho uma nova tecnologia está tomando e seu impacto na vida de pessoas e organizações, pois, segundo Day, Schoemaker e Gunther (2003) a turbulência e as incertezas dos mercados futuros com relação a novas tecnologias confundem as abordagens de pesquisa dispostas a avaliar mercados estabelecidos, onde raras vezes há precedentes ou histórias para estudo. Neste sentido, quando as incertezas são intoleravelmente altas, existem três premissas: 1) difusão e adoção (cada tecnologia emergente se difundirá a uma razão e a um ritmo diferentes em seus mercados potenciais); 2) exploração e aprendizagem (a vantagem advém de uma antecipação informada, ou seja, ênfase em uma rápida aprendizagem resultante de uma série de

sondagens de mercado); e 3) triangulação (a capacidade de absorver incerteza e antecipar oportunidades é aumentada por processos divergentes de pensamento, que aumentam a gama de possibilidades) e *insights* (proveem de um processo de triangulação que procura a convergência de conclusões entre métodos diferentes) (DAY, SCHOEMAKER E GUNTHER, 2003).

Não existe um modelo ou paradigma estabelecido para a gestão de tecnologias emergentes – mas, no melhor dos casos, uma gama diversa de perspectivas e de abordagens. Ao exercerem tremendas forças gravitacionais na organização, estas rápidas e novas tecnologias pedem modelos e métodos diferentes de gestão (DAY; SCHOEMAKER; GUNTHER, 2003).

Um dos aspectos mais confusos das tecnologias emergentes é o fato de os padrões de uso e o comportamento dos consumidores serem exploratórios e estarem em formação, ao passo que o conhecimento do mercado é escasso, e a estrutura de concorrência, embrionária (DAY, SCHOEMAKER, GUNTHER, 2003).

Desta forma, antes de gerir novas tecnologias, é preciso entender como se dá o processo de adoção destas novas tecnologias, a fim de verificar seu impacto no cotidiano de pessoas e organizações. Santos (2007) comenta que dentre os principais modelos de adoção de TIC's, a Teoria da Difusão da Inovação propõe que a adoção e difusão de inovações tecnológicas é motivada pelo aumento da eficiência e desempenho organizacional, conhecida como perspectiva de escolha estratégica, onde a adoção de TIC's precisa ser investigada utilizando-se uma combinação de diferentes abordagens que supram possíveis lacunas existentes em cada abordagem.

Marques (2008) coloca que o modelo de análise de tecnologias, conhecido como paradigma tecno-econômico, preconiza a compreensão da relação entre as dimensões tecnológica e econômica como um conjunto de impactos fundamentais para o desenvolvimento econômico. Este paradigma ganhou caráter prospectivo, uma vez que ao trabalhar com cenários futuros, que poderão se confirmar ou não, e que as formas que as ferramentas atuais de avaliação tecnológica tentam prever tendências da evolução se dão através de parâmetros técnicos e por suas consequências econômicas.

Realizar avaliação de esforços de Pesquisa e Desenvolvimento - P&D é um processo complexo que envolve, dentre outras questões, a capacidade de lidar com a natureza incerta do avanço do conhecimento e a representação de seus impactos na sociedade, a partir de uma visão subjetiva do avaliador e dos atores envolvidos. Estudos voltados à

mensuração de impactos sociais de programas tecnológicos, bem como atividades de P&D, são pouco frequentes na literatura, comparados às dimensões econômica e ambiental (BONACELLI; ZACKIEWICZ; BIN, 2003)

Uma das razões para a preocupação com a previsibilidade da trajetória de um novo desenvolvimento tecnológico ocorre em função de impactos negativos significativos de algumas tecnologias anteriores. Neste contexto, há três maneiras de influência dos riscos: **conhecimento do risco**, onde as possibilidades de nova aplicação tecnológica não são plenamente dominadas; **uso da tecnologia diretamente no objeto de aplicação**, onde por mais que os riscos sejam conhecidos, uma ação fora do controle pode provocar danos graves; e **efeitos de ordem superior à tecnologia** ou **efeitos negativos indiretos**, ou seja, aqueles danos não previstos, que ocorrem fora da análise tecnológica considerada. O expressivo poder de impacto de novas tecnologias, significativamente permeáveis em diversos setores da economia e que carregam uma capacidade de transformação revolucionária, não é contemplado em modelos de análise tradicionais, geralmente bidimensionais, ou seja, não há um modelo suficientemente consistente, que incorpore novas dimensões da complexidade do cenário de desenvolvimento tecnológico atual, que respondam a atual necessidade de que uma nova tecnologia gere impactos econômicos e que estes gerem impactos nas relações sociais e ambientais. Novas relações em outras dimensões de análise são requisitos do contexto tecnológico que somente modelos de análise multidimensionais podem atender (MARQUES, 2008).

Desta forma, para que se possa entender o dimensionamento e os efeitos da tecnologia, é preciso pensar sistematicamente, é preciso analisar esta tecnologia como um sistema, identificando sua composição, suas relações, atores, ou seja, é preciso ter uma visão sistêmica, que segundo Moretto, Galdo e Kern, (2010) é onde os sistemas tecnológicos passam a constituir sistemas sociotecnológicos, que são um tipo de sistema complexo, auto organizado, cujo funcionamento depende de uma colaboração dinâmica que envolve pessoas e agentes artificiais; é o entendimento dos aspectos técnicos e sociais como partes de um mesmo sistema.

Neste sentido, uma forma de entender as partes de um sistema, é separá-lo em dimensões, ou seja, se analisarmos uma nova tecnologia, que se encontra em um estado emergente de desenvolvimento, estas são normalmente vistas sob a relação direta entre as dimensões tecnológicas e a dimensão econômica, normalmente desprezando, de certa forma, outras possíveis dimensões (MARQUES, 2008). Sendo assim, é preciso

analisar a adoção de uma tecnologia nas suas mais diversas dimensões, a fim de avaliar seu real impacto.

A tecnologia escolhida para análise foi a certificação digital, uma vez que há uma grande preocupação com segurança da informação, principalmente no que concerne às transações eletrônicas, cada dia mais presentes no cotidiano das pessoas.

Martini (2008) aponta uma lacuna existente em relação a inexistência de pesquisas na área das ciências sociais, que tratem da evolução da certificação digital no país, uma vez que existem apenas pesquisas em relação a parte tecnológica, algoritmos criptográficos, sendo necessário um estudo e avaliação do cenário brasileiro, o que foi constatado também nesta pesquisa, a partir da realização de uma revisão sistemática das publicações científicas no Brasil.

Diante das considerações tecidas, a justificativa desta pesquisa baseia-se nas garantias que a certificação digital vem a oferecer, ou seja, segurança, confidencialidade, integridade, autenticidade das informações e comunicações, e ainda validade jurídica, além dos resultados subjacentes oferecidos, que seja, agilidade de processos à economia verde. Reafirmando uma necessidade destes requisitos para a sociedade de uma forma geral e que o número de aplicações está crescendo a cada ano e aos poucos vai sendo disseminado, é preciso perceber e entender os efeitos desta nova tecnologia na sociedade e nas organizações, bem como, verificar os caminhos e resultados esperados para o futuro desta tecnologia.

## 1.4 DELIMITAÇÃO DA PESQUISA

Esta pesquisa visa analisar o impacto da certificação digital no Brasil, e para tanto foram consideradas as perspectivas de especialistas indicados pelo ITI, entidade responsável pela cadeia de confiança da certificação digital no Brasil.

Por tanto, buscou-se abranger especialistas de diversos órgãos que já utilizam certificação digital ICP-Brasil há algum tempo, ou que estejam ligadas à sua implantação, sendo indicados pelo ITI, 27 especialistas com quem aplicamos as entrevistas semiestruturadas.

Neste sentido, a presente pesquisa restringe-se a:

- Abordar o estudo sob o enfoque da visão sistêmica;
- Restringe-se ainda a analisar o impacto da certificação digital ICP-Brasil, com base na visão de especialistas, não aprofundando-se no processo de difusão da mesma.

Dessa forma, não faz parte de escopo desta pesquisa analisar impacto sobre a visão do usuário final do cerificado digital.

## 1.5 ADERÊNCIA DO TEMA AO PPEGC

O presente trabalho de dissertação enquadra-se na área de concentração Gestão do Conhecimento, do Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento (PPEGC), na linha de pesquisa "Gestão do Conhecimento, Empreendedorismo e Inovação Tecnológica", que tem por objetivo "estudar o comportamento individual frente ao fenômeno de geração de conhecimento da sociedade da informação e sua utilização inovadora na busca do desenvolvimento pessoal do bem estar social e da geração de renda" (EGC, 2014).

Utilizando de processos de análise já definidos para outras tecnologias e associando as teorias de Engenharia e Gestão do Conhecimento, neste caso a visão sistêmica, através do modelo CESM, esta pesquisa se configura numa combinação de abordagens que permitam a análise de impacto da certificação digital ICP-Brasil.

Esta pesquisa possibilita a identificação de oportunidades à organizações e governos na identificação de conhecimento necessário para a identificação de processos de adoção de novas tecnologias, bem como o impacto destas, fomentando, desta forma, novos processos de inovação.

Outro ponto de aderência ao programa se refere ao emprego das metodologias e técnicas específicas na combinação de modelos que representem uma possibilidade de descoberta do conhecimento existente nas estratégias adoção de inovações em Tecnologia de Informação e Comunicação, bem como um processo de identificação de hipóteses de futuro de novas tecnologias e seu impacto para a sociedade.

Cabe ressaltar que a previsão de futuro e a análise de impacto são intrínsecas aos indivíduos, ou seja, é necessário um modelo de conhecimento que consiga capturar o conhecimento empírico dos indivíduos e que resulte em informações para o processo de tomada de decisão.

Considera-se que informações devem ser fisicamente mantidas em segurança para evitar o acesso e as possíveis disseminação e utilização por fontes não autorizadas, uma vez que estas são as principais preocupações que influenciam diretamente as chances de um cliente adotar tecnologias e conduzir negócios por meio da web (BALTZAN E PHILLIPS, 2012).

Destaca-se que a pesquisa tem caráter interdisciplinar, uma vez que envolve teorias da Administração, Ciência da Informação, Ciência da Computação, Ciências Sociais, Gestão da Inovação, promovendo a integração dos resultados obtidos pelo entendimento e pela busca de soluções de um problema através da articulação de disciplinas, o que justifica a aderência ao programa de Pós-Graduação em Engenharia e Gestão do Conhecimento.

## 1.6 CARACTERIZAÇÃO DA PESQUISA

Considerando que é preciso compreender a relação entre as dimensões que envolvem a análise de tecnologias, bem como os riscos envolvidos na trajetória desta tecnologia e seus impactos (MARQUES, 2008), esta pesquisa utiliza como visão de mundo a visão sistêmica e configura-se: quanto à natureza como uma **pesquisa aplicada**; quanto à abordagem, como **pesquisa qualitativa**; quanto aos objetivos, como **pesquisa exploratória e descritiva**; quanto à coleta de dados estase deu por meio de entrevistas semiestruturadas com especialistas. E os dados foram analisados usando **análise de conteúdo** e **análise temática**, conforme apresentado mais detalhadamente no capítulo de procedimentos metodológicos.

## 1.7 ESTRUTURA DAPESQUISA

Esta pesquisa está estruturada em cinco capítulos, descritos a seguir.

a) O **primeiro capítulo** diz respeito à introdução, onde constam o tema e o problema, os objetivos geral e específicos, bem como a justificativa, a aderência do tema ao PPGEGC, a caracterização e a estrutura da pesquisa;
b) No **segundo capítulo** encontra-se a revisão de literatura, onde são desenvolvidos os principais conceitos que permitiram o embasamento teórico da pesquisa, que são: Sociedade do conhecimento, Tecnologias de Informação e Comunicação, Modelos de adoção de inovações tecnológicas, e Análise de impacto;
c) No **terceiro capítulo** são apresentados os procedimentos metodológicos utilizados para desenvolver a pesquisa e a descrição da análise de conteúdo utilizada – análise temática;
d) No **quatro capítulo** é apresentada a análise e discussão dos resultados;
e) No **quinto capítulo** são apresentadas as considerações finais e estudos futuros.

Por fim, são disponibilizadas as referências utilizadas na pesquisa e os apêndices.

# 2 REVISÃO DE LITERATURA

A finalidade deste capítulo é apresentar e discutir as principais bases conceituais que fundamentam esta dissertação, desta forma, o capítulo está organizado da seguinte maneira: 2.1 **Sociedades do Conhecimento**; 2.2 **Tecnologias de Informação e Comunicação**; 2.3 **Infraestrutura de Chaves Públicas Brasileira e a Certificação Digital**; 2.4 **Modelos de adoção de inovações tecnológicas**; 2.5 **Análise de impacto**.

A intenção não é esgotar os temas tratados, mas apresentar um panorama geral das teorias e discussões na área, visando direcionar o atendimento dos objetivos propostos nesta pesquisa.

## 2.1 SOCIEDADES DO CONHECIMENTO

Desde a formação dos agrupamentos sociais, o conhecimento já significava domínio dos processos de plantar, construir e/ou manufaturar, hoje, ele é visto como bem e as necessidades são o domínio de manipular, estocar e transmitir gigantescas e crescentes quantidades de informação, o que configura a sociedade do conhecimento, que é descrita por Squirra (2005) como uma combinação das configurações e aplicações da informação com as tecnologias da comunicação em todas as suas possibilidades, ou seja, traz consigo a velocidade do tempo real, com vastas possibilidades de controle, armazenamento e acesso a múltiplos conjuntos de informações, impactando na produtividade das economias nacionais e na busca pela competitividade, mas que esta mesma sociedade gera formas próprias de exclusão, onde há os que têm e os que não têm acesso a informação, resultando numa divisão digital.

O conhecimento passou de uma função auxiliar de poder financeiro à sua própria essência, e em razão disso a batalha pelo seu controle e o controle dos meios de comunicação têm se acirrado. Uma vez que o conhecimento é a fonte de poder de mais alta qualidade e a chave para uma futura “mudança de poder”, ele é visto como um recurso-chave e fonte de vantagem competitiva presente no processo de inovação (Reis, 2008).

Neste contexto, uma organização do conhecimento é aquela organização que possui informações e conhecimentos que lhe conferem uma vantagem que lhes permite agir com inteligência, criatividade e

esperteza, ou seja, é uma organização em constante aprendizado e inovação, o que faz com que tal organização possa estar preparada para adaptações com antecedência, criando significados, construindo conhecimentos e tomando decisões (CHOO, 2006).

Com o advento do novo modelo socioeconômico, baseado no conhecimento, que passa a ser tratado como bem, surge segundo Araújo (2009), uma preocupação com a segurança destes ativos intangíveis, ou seja, o mundo está em processo de transformação estrutural há pelo menos duas décadas, configurando-se em um processo multidimensional, que está associado à emergência de um novo paradigma tecnológico, baseado nas TIC's, que começaram a tomar forma nos anos 60 e que se difundiram de forma desigual por todo o mundo, e que são particularmente sensíveis aos efeitos dos usos sociais da própria tecnologia. Sabe-se que não é a tecnologia que determina a sociedade, é a sociedade que dá forma à tecnologia de acordo com as necessidades, valores e interesses das pessoas que as utilizam, ou seja, tecnologia é condição necessária, mas não suficiente para a emergência de uma nova forma de organização social baseada em redes (CASTELLS e CARDOSO, 2005)

Neste sentido, as tecnologias de compartilhamento de informações, que permitem que a sociedade compartilhe informações de forma intuitiva, principalmente mediadas por computador, geram uma complexa rede de comunidades, denominada como sociedade em rede. Esta rede, segundo a Lei de *Metcalfe*, tem um valor potencial, na relação potencial de interações da informação entre entidades ou nós em rede.

Desta forma, nossa maneira de ser se dispõe antes pela difusão e compartilhamento da informação e do conhecimento, do que pelo sigilo das mesmas (MARTINI, 2013). Ao discursar sobre o modo de ser, comunicar e compartilhar informação, e a questão ética destas relações, Martini (2013) ainda coloca que:

> [...] não compartilhamos informação por que uma Lei impositiva nos obriga ou por que regras ou preceitos morais nos impeliriam. Estes dois estágios, por assim dizer, são apenas e somente epifenômenos. São a *posteriori*, só podem interferir senão de forma secundária. (MARTINI, 2013, p.5)

Neste contexto, com o advento das redes sociais surge um novo desafio para nações, sociedade e empresas, uma vez que nada mais é

segredo: como conter informações estratégicas, manter sigilo, preservar a segurança de dados, como impedir vazamento de dados? Não existem ainda respostas consideráveis; os meios acadêmicos apenas iniciaram estudos das infinitas implicações sociais, empresariais e eventuais ameaças de Estado dessa interconectividade plena (FEBRABAN, 2013).

Quando se discute sobre proteção de conhecimento, Araújo (2009) coloca que não há discussões a respeito e nem mesmo está previsto em legislação, mas que as mesmas regras de segurança de informação, servem para a segurança de conhecimento, exemplo: norma ABNT NBR ICO/IEC 17799 (2002), que define segurança da informação como preservação da confidencialidade, integridade e disponibilidade da informação. Este autor dialoga ainda sobre como reduzir riscos[1] residuais e como controlar a tensão entre compartilhar ou proteger conhecimento, uma vez que a compreensão de como controlar conhecimento em um ambiente competitivo e globalizado, onde é necessária contínua inovação e aprendizagem, é uma tarefa delicada. Apresenta alguns autores que defendem a ideia de que a proteção do conhecimento deveria ser vista como uma questão de proteção de patrimônio, e não só como uma questão estratégica.

No que concerne à preservação de conhecimento Araújo (2009) apresenta diversas discussões a respeito da dificuldade de preservar conhecimento, uma vez que ele está presente em diferentes dispositivos e diferentes ambientes, seja nas organizações ou fora delas, devendo ser tratado juntamente com os processos de inovação. O grande desafio para a gestão da segurança do conhecimento é encontrar formas de harmonizar questões como: vazamento do conhecimento *versus* retenção, proteção *versus* compartilhamento, bem como identificar o conhecimento que deve ser protegido, quais procedimentos para protegê-lo, quando estes procedimentos devem ser aplicados, quais os custos para tanto, dentre outras questões (ARAUJO, 2009).

Araújo (2009) coloca que as organizações são proprietárias dos recursos de conhecimento organizacional, portanto, devem manter tais recursos protegidos de uso não autorizado, de alterações, de atos de vandalismo e de sabotagem, mesmo que algumas delas acreditem que a inclusão de medidas de segurança em seus programas, possam impactar

[1] Araújo (2009) adota as definições de (1) risco de Tittel et.al. (2003) e de (2) ameaça de Krutz e Vines (2001) como a: (1) "possibilidade de que uma ameaça específica venha explorar uma vulnerabilidade específica e causar dano a um ativo", onde ameaça é (2) "a presença de todo o evento potencial que causar um impacto indesejável".

o espírito de compartilhamento de conhecimento. Estas organizações devem realizar análise de riscos, que são atividades que identificam ativos de conhecimento, quantificam o impacto de ameaças, auxiliam na elaboração de orçamento para segurança, e ajudam a integrar necessidades e objetivos da política de segurança de conhecimento com os objetivos e intenções de negócio da organização.

Deste modo, uma das TIC's utilizadas na gestão de segurança de informações, é a certificação digital, portanto, na próxima seção serão apresentadas discussões sobre Tecnologias de Informação de Comunicação.

## 2.2 TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Esta seção tem por objetivo apresentar conceitos e definições sobre as TIC’s, inserindo a certificação digital como uma TIC utilizada na gestão de segurança de informações.

### 2.2.1 Conceitos e Definições

Tecnologia significa um conjunto de processos pelos quais uma organização transforma mão de obra, capital, materiais e informação em produtos e serviços de grande valor, fazendo com que seu conceito ultrapasse a engenharia e a produção, se estendendo ao marketing, investimento e processos de administração. Ao se considerar a inovação como uma mudança destas tecnologias, onde o progresso tecnológico pode andar, e frequentemente anda, mais depressa do que os fabricantes necessitam e esperam, significa considerar que a relevância e a competitividade de abordagens tecnológicas distintas podem alterar diferentes mercados ao longo do tempo (CHRISTENSEN, 2012).

A tecnologia está associada a impactos socioeconômicos sobre uma comunidade, resultantes da aplicação de novos materiais, novos processos de fabricação, novos métodos e novos produtos, onde para que uma tecnologia criada seja transformada em inovação, ela deve ser produzida pelos agentes econômicos (as empresas), disponibilizada para a sociedade e ser aceita pela mesma, desta forma, o desenvolvimento tecnológico pode ser alcançado tanto pela criação de novas tecnologias quanto pela utilização mais eficaz de tecnologias já existentes (REIS, 2008)

Neste sentido, surgem as TIC’s que são tecnologias que associam a informação e a comunicação, necessárias para o processamento de dados, em particular, através do uso de *hardwares* e *softwares*, para converter, armazenar, proteger, processar, transmitir e recuperar informações. São recursos tecnológicos que intermediam as relações sociais.

Segundo Afonso et.al (2003) TIC's são procedimentos, métodos e equipamentos utilizados para processar informação e comunicar, e que se dividem em três áreas de aplicação: computacional, comunicação e controle e automação.

Farias (2013) comenta que as TIC’s podem ser consideradas como um conjunto de recursos tecnológicos, que permitem maior facilidade no acesso e na disseminação de informações.

As TIC’s, assim como sua aplicação às atividades relacionadas ao gerenciamento do conhecimento, constituem o cerne das questões de adaptação da empresa em um ambiente dinâmico e interativo, onde a tecnologia deve ser aplicada de forma integrada e sistêmica à organização (ANGELONI, 2002).

O acesso à informação e à comunicação e o desenvolvimento dos recursos proporcionados pelas TIC's determinam cada vez mais o desenvolvimento econômico e social. Fatores específicos e o porte das empresas têm influência importante na adoção e no uso destas tecnologias, ou seja, o desenvolvimento das TIC's e sua rápida difusão pelos canais de comunicação abrem novas possibilidades de ganhos econômicos e de progresso social através de um maior compartilhamento de informações e serviços entre indivíduos e grupos de interesse comum (OCDE, 2003).

Neste contexto, a competitividade global é ditada principalmente pela velocidade, qualidade e eficiência, seja das decisões, das implementações ou das comunicações, onde a infraestrutura de TIC’s permite a comunicação entre pessoas e recursos, devendo ser bem projetada e dimensionada (NAKAMURA e GEUS, 2007).

Uma vez que as TIC’s permitem uma maior interconectividade entre indivíduos, surgem questões como segurança, ética e privacidade de informações, que serão apresentadas na subseção seguinte.

### 2.2.2 Segurança da informação

A presente subseção tem como objetivo apresentar algumas discussões a respeito de segurança, ética e privacidade de informações, a fim de inserir a certificação digital como ferramenta fundamental neste campo.

A internet é hoje um dos principais mecanismos do comércio, da indústria, do ensino e, ainda, de governança, ela cria uma rede complexa de usabilidade de diversas tecnologias e sistemas em larga escala, e consequentemente, apresenta uma suscetibilidade às ameaças, tornando críticas questões de segurança, principalmente no que concerne ao comércio eletrônico.

Cada dia mais, as redes sociais e a facilidade de compartilhamento desafiam fronteiras, e consequentemente, os gestores a se preocuparem com o sigilo de informações, além da segurança. Surgem preocupações com bloqueios de acesso à internet ou vazamento

de dados, acesso não autorizado, monitoramento de conteúdo, dentre outras questões, uma vez que há uma interconectividade plena, não havendo nenhuma previsão de como estas questões podem impactar organizações e países. Desta forma, é indispensável tomar conhecimento dos riscos a que empresas e países estão expostos, tentando criar mecanismos para mitigar possíveis danos (FEBRABAN, 2013).

No mundo da informação deve-se ter em mente que a segurança deve ser contínua e evolutiva, e que alguns fatores devem ser considerados: entender a natureza dos ataques é fundamental (vulnerabilidade por falha no projeto ou de implementação); novas tecnologias trazem consigo novas vulnerabilidades; novas formas de ataques são criadas; aumento da conectividade resulta em novas possibilidades de ataques (aumento de curiosos e possibilidade de disfarce); existência tanto de ataques direcionados quanto de ataques oportunísticos (ataques direcionados não são feitos de maneira aleatória e são mais agressivos e provocam maiores perdas); defesa é mais complexa do que o ataque (*hacker* ataca um ponto de falha, a defesa exige que todos os pontos sejam defendidos); e aumento dos crimes digitais (limites geográficos são transpostos e legislação para crimes digitais está em fase inicial) (NAKAMURA e GEUS, 2007).

Turban, Raiber e Potter (2007) colocam que o mau uso das tecnologias está à frente das discussões e que a diversidade e o uso cada vez mais difundido de aplicações criaram diversos aspectos éticos categorizados em 4 tipos: *privacidade* (envolve coleta, armazenamento e disseminação de informações sobre pessoas. É o direito de determinar até que ponto as informações sobre uma pessoa podem ser coletadas e/ou comunicadas. Este direito não é absoluto, podendo prevalecer sobre ele o direito público); *exatidão* (envolve autenticidade, fidelidade e correção de informações coletadas e processadas); *propriedade* (envolve propriedade e valor das informações); e, *acessibilidade* (envolve questões de acesso, permissões e precificação).

Em relação aos sistemas de informação, Turban, Raiber e Potter (2007) inserem a definição de controles de sistemas de informação, que são os procedimentos, dispositivos ou softwares destinados a evitar o comprometimento de um sistema. Nestes sistemas, existem dois tipos de ameaças: as involuntárias (erros humanos, riscos ambientais e falhas no sistema de computação) e voluntárias (espionagem ou invasões; sabotagem ou vandalismo; roubo; ataques de *software*, dentre outros). Neste sentido, apresentam duas categorias de controle de proteção: controles gerais (têm o objetivo de proteger o sistema) e controles de aplicativos (têm o objetivo de proteger aplicativos específicos).

Os controles gerais se dividem em pelo menos cinco tipos: 1) **Controles físicos** (é a primeira linha de defesa e normalmente a mais fácil de construir, protegendo instalações e recursos computacionais da maioria dos perigos naturais e humanos); 2) **Controle de acesso** (é a restrição imposta a usuários não-autorizados, que pode ser através de senha, *smartcard* ou *token* ou controles biométricos); 3) **Controle de segurança de dados** (é a proteção de dados contra a revelação acidental ou intencional à pessoas não-autorizadas ou modificação ou destruição não-autorizada; o que inclui questões de confidencialidade dos dados, controle de acesso, natureza vital dos dados e integridade dos dados); 4) **Controle de Comunicação** (rede); 5) **Controles administrativos** (diz respeito a definição de diretrizes e o monitoramento do cumprimento dos demais controles (TURBAN, MCLEAN E WETHERBE, 2004).

Neste sentido, Martini (2013) coloca que as políticas de segurança são basicamente *policies* para o controle do acesso à informação e à dados de algum tipo, onde um dos principais mecanismos de segurança hoje é o certificado digital, capaz de garantir a autenticidade, confidencialidade, integridade e o não repúdio de transações e informações.

Neste sentido, uma questão importante a se considerar é que do lado oposto do compartilhamento de informações, bem como de seu uso, há a questão do sigilo, onde sigilo é diferente de segredo, ou seja, sigilo é uma *retenção metódica e estruturada* de uma parte ou peça de um conjunto de informações que se produze mantém em uma organização. Uma política de sigilo visa discriminar e separar o acesso de informações a pessoas ou grupos, através de plataformas tecnológicas, como criptografia, *hardware* criptográfico, dentre outros, a fim de evitar o uso indevido ou perverso da retenção da informação, qual seja ela, uma vez que a manipulação e o uso do sigilo podem levar a graves consequências no plano das relações interpessoais no mundo do trabalho (MARTINI, 2013).

Em 1976, surgiu um dos principais recursos de segurança de informações digitais, a criptografia de chaves públicas, com Diffie e Hellman, que permitiu, dentre outras características, o estabelecimento da assinatura digital de documentos eletrônicos. Esta tecnologia exigia outro mecanismo que permitisse a correlação entre chaves públicas, dando origem a proposta de Kohnfelder, em 1978, a certificação digital, também denominada identidade digital. O certificado digital ou identidade digital “é um arquivo digital que, como os demais documentos tradicionais de identificação, além dos dados do indivíduo

ou entidade, possuem também uma Chave Pública do assinante" (MONTEIRO E MIGNONI, 2007).

No Brasil, foi criada em 2001 a Infraestrutura de Chaves Públicas - ICP-Brasil, entidade que regulamenta todas as questões relacionadas aos certificados digitais com validade jurídica no Brasil.

Na próxima seção, serão detalhados estes dois últimos itens: ICP-Brasil e certificação digital, com maior profundidade.

## 2.3 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA E A CERTIFICAÇÃO DIGITAL

Esta seção tem por objetivo apresentar conceitos e definições que envolvem a certificação digital e a Infraestrutura de Chaves Públicas ICP-Brasil.

### 2.3.1 Criptografia e a certificação digital

Burnett e Paine (2002) colocam que, no passado, a segurança de informações era simplesmente uma questão de trancar uma porta ou armazená-las em armários com chave. Na sequência surgiram os cofres que necessitavam de um código de acesso (senha). Com as novas mídias, apesar de possuírem finalidades semelhantes, a questão da proteção de dados não é tão simples. No meio digital, a privacidade dos dados é a "fechadura da porta"; a integridade é o "alarme"; e o não-repúdio ou irretratabilidade é uma "imposição legal que orienta e impele as pessoas a honrar as suas palavras" (BURNETT E PAINE, 2002).

Segundo Monteiro e Mignoni (2007, p.5), "o nível de segurança das informações estabelecidas por criptografia depende do tamanho da chave, onde quanto mais *bits* uma chave possuir, maior a dificuldade de ser descoberta".

Neste sentido, Burnett e Paine (2002) colocam que a criptografia é "uma das ferramentas mais importantes para a proteção dos dados" (p.8), pois "não é a única ferramenta necessária para assegurar a segurança de dados, nem resolverá todos os problemas de segurança" (p.10). Ela "converte dados legíveis em algo sem sentido, com a capacidade de recuperar os dados originais a partir destes dados sem sentido" (p.11). É considerada ainda como:

> [...] uma ciência que tem importância fundamental para a segurança da informação, ao servir de base para diversas tecnologias e protocolos, tais como a infraestrutura de chaves públicas (*Public Key Infrastructure – PKI*), [...]. Suas propriedades – sigilo, integridade, autenticação e não-repúdio – garantem o armazenamento, as comunicações e as transações seguras, essenciais no mundo atual. (Nakamura e Geus, 2007, p. 301)

Monteiro e Mignoni (2007) definem criptografia como um algoritmo/cifragem que visa “esconder/ocultar” de forma embaralhada informações sensíveis, tornando-as incompreensíveis à pessoas não autorizadas. Ela pode ser de dois tipos: criptografia simétrica e criptografia assimétrica. A *criptografia simétrica* utiliza somente uma chave para cifrar e decifrar um texto, onde tanto emissor quanto o receptor da mensagem deve conhecer a chave utilizada; já a *criptografia assimétrica* ou de chave pública, utiliza um par de chaves distintas (chave pública e chave privada) e cada usuário possui seu par de chaves, esta última permite o uso da assinatura digital, que é um algoritmo de autenticação que possibilita saber que um documento foi assinado por um determinado autor.

Neste contexto, surge a certificação digital, que segundo Monteiro e Mignoni (2007) utiliza como base a tecnologia de criptografia de chave pública, onde esta é armazenada no certificado, enquanto a chave privada é guardada sigilosamente pelo assinante.

Para Silva et.al. (2011) certificação digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos.

Já o certificado digital é um arquivo de computador que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido, mais uma chave pública referente à chave privada desta entidade (SILVA et.al., 2011).

Segundo o ITI (2013), certificado digital é um arquivo eletrônico armazenado em uma mídia digital que contém os dados do seu titular, pessoa física ou jurídica, utilizado para relacionar tal pessoa a uma chave criptográfica que atesta a identidade, garantindo confidencialidade, autenticidade e o não repúdio nas transações comerciais e financeiras por elas assinadas, bem como a troca de informações com integridade, sigilo e segurança. Desta forma, o certificado digital ICP-Brasil identifica quem somos para as pessoas e para os sistemas de informação.

A certificação digital é uma tecnologia auxiliar que permite que soluções tecnológicas digitais possam operar de forma segura, atestando a identidade do usuário, garantindo confidencialidade, autenticidade e o não repúdio nas transações assinadas eletronicamente, além de também permitir a troca de informações com integridade, sigilo e segurança (IGTI, 2014)

Para emitir certificados digitais confiáveis e regulamentados, é necessária a criação de um sistema de certificação, ou seja, deve ser

adotada uma Infraestrutura de Chaves Públicas – ICP, como será apresentado na próxima subseção.

### 2.3.2 Infraestrutura de Chaves Públicas

Uma infraestrutura de chaves públicas é:

> [...] um órgão ou iniciativa, pública ou privada, que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de acreditação e confiança em transações entre partes que utilizam certificados digitais. [...] A principal função da ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública (SILVA, et.al., 2011, p. XI).

No Brasil o responsável pela emissão de certificados chancelados, ou seja, que pertencem a uma cadeia de confiança, é o Instituto Nacional de Tecnologia da Informação – ITI, que é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, sendo a primeira autoridade da cadeia de certificação, a Autoridade Certificadora Raiz - AC Raiz.

Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Sua principal linha de ação é a popularização da certificação digital ICP-Brasil e a inclusão digital, atuando sobre questões como sistemas criptográficos, hardware compatíveis com padrões abertos e universais, convergência digital de mídias, desmaterialização de processos, entre outras (ITI, 2013).

O sistema nacional de certificação digital no Brasil teve origem através da Medida Provisória 2.200-2 de 24 de agosto de 2001. O que representa uma infraestrutura pública, mantida e auditada por órgão público, no caso, o ITI, que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil.

O Comitê Gestor da ICP-Brasil, por sua vez, é a autoridade gestora das políticas relacionadas ao tema Tecnologia da Informação. O Comitê é composto por cinco representantes da sociedade civil, integrantes de setores interessados designados pelo Presidente da

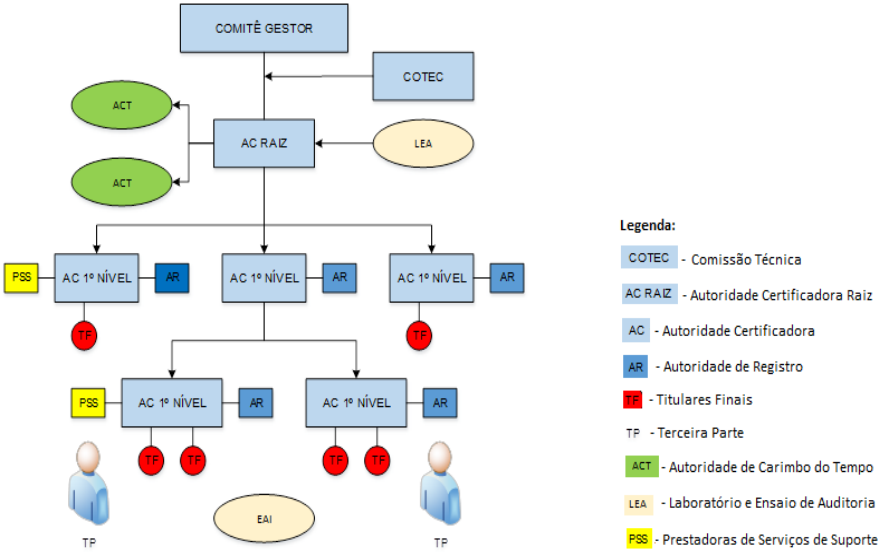
República e um representante do Ministério da Justiça; Ministério da Fazenda; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Casa Civil da Presidência da República e Gabinete de Segurança Institucional da Presidência da República. (ITI, 2013)

O Comitê Gestor além de atuar na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil atua também nos aspectos de normatização e nos procedimentos administrativos, técnicos, jurídicos e de segurança, que formam a cadeia de confiança da ICP-Brasil.

Uma ICP, segundo Monteiro e Mignoni (2007), é uma organização envolvendo componentes (Autoridade Certificadora – AC; Autoridade de Registro – AR; etc.), um conjunto de serviços necessários para uso de tecnologias baseadas em Chave Pública, usadas em grande escala. Essa organização se configura numa estrutura, onde a confiança é mais um item de segurança a ser analisado e auditado.

Segundo o ITI, a ICP-Brasil, é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Onde se observa que o modelo adotado foi o de certificação com raiz única (Figura 4).

**Figura 4: Organograma da ICP-Brasil**




Fonte: Bertol (2009)

A cadeia de confiança de certificação digital ICP-Brasil se configura na estrutura hierárquica existente entre os componentes da ICP-Brasil: a AC Raiz, as AC's de primeiro nível e segundo nível, as AR's (Autoridades de Registros), repositórios de certificados, e, finalmente, o usuário final, ou seja, cada ator da cadeia certifica o próximo, tendo a AC Raiz como âncora de confiança da cadeia, ou seja, seu certificado é auto assinado.

A ICP-Brasil conta no ano de 2013 com doze Autoridades Certificadoras de 1º nível – AC; trinta e sete Autoridades Certificadoras de 2º nível e cerca de 282 Autoridades de Registro – AR, e outras em fase de credenciamento. Em 2012 foram emitidos 2.100.235 certificados digitais e este número vem crescendo. (BOLETIM DIGITAL, 2013)

Alguns fatores contribuíram para a consolidação da certificação digital ICP-Brasil, como: a diversidade de aplicações nos setores público e privado, que utilizam o conjunto de regras rígidas de segurança proposto por essa certificação (o que norteia a relação de confiança estabelecida entre as entidades da estrutura organizacional da ICP-Brasil), e a validade jurídica por ela proporcionada (IGTI, 2014)

No Brasil, os certificados ICP-Brasil, segundo o ITI, são classificados quanto à sua aplicabilidade e quanto aos requisitos de segurança.

Em relação à aplicabilidade existem três tipos de certificados:

- **Certificado do Tipo A**: ou certificados de Assinatura Digital, são utilizados para assinatura de documentos, transações eletrônicas, etc. tendo como meta provar a autenticidade e a autoria por parte do emissor/autor, garantindo também, a integridade do documento;
- **Certificado do Tipo S**: ou certificados de Sigilo, são utilizados somente para proporcionar sigilo ou criptografia de dados. São os certificados digitais utilizados para o envio e/ou armazenamento destes documentos sem expor o seu conteúdo; e
- **Certificado de Tempo (T)**: também conhecido como *time-stamping*, é o serviço de certificação da hora e do dia em que foi assinado um documento eletrônico, com identidade do autor.

Quanto a segurança, os certificados são classificados conforme mostra a Quadro 1.

**Quadro 1: Classificação dos certificados quanto à segurança**

| Tipo | Tamanho da chave (bits) | Geração do par de chaves | Validade máxima do certificado |
|---|---|---|---|
| **A1/S1** | 2048 | Software | 1 ano |
| **A2/S2** | 2048 | Hardware | 2 anos |
| **A3/S3** | 2048 | Hardware | Até 5 anos |
| **A4/S4** | 4096 | Hardware | Até 6 anos |
| **T3** | 2048 | Hardware | Até 5 anos |
| **T4** | 2048 | Hardware | Até 6 anos |

Fonte: Adaptado da Cartilha ICP-Brasil, 2012.

Sobre a validade, esta se configura como uma forma também de segurança, pois exige a revalidação periódica.

### 2.3.3 Breve Histórico sobre a Infraestrutura de Chaves Públicas Brasileira

As primeiras discussões sobre a criação de uma infraestrutura de chaves públicas para o governo iniciaram em 1999, com o Grupo de Trabalho de Segurança da Informação da Câmara Técnica de Serviços de Rede – GT3/CTSR, sob a gerência da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Para tanto, foi instituído o Grupo de Trabalho Interministerial (GTI) através da Portaria nº 043 da Casa Militar da Presidência da República – CMPR, tendo como objetivo principal propor aos órgãos do Poder Executivo Federal a adoção de instrumentos jurídicos, normativos e organizacionais que os capacitassem científica, tecnológica e administrativamente a assegurar o sigilo, a integridade, a autenticidade, a irretratabilidade e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis. Em março de 2000 foi submetido ao Comitê Gestor de Segurança da Informação – CGSI a proposta de criação da Infraestrutura de Chave Pública do Poder Executivo – ICP-Gov, ou Infraestrutura de Chaves públicas do Poder Executivo Federal (AGP, 2000).

Em 2000, foi criado o Governo Eletrônico Brasileiro e o GTI passou a ser denominado Grupo de Trabalho em Tecnologia da Informação (GTTI), por meio do Decreto de 3 de abril de 2000, com o objetivo de apresentar propostas de soluções, normas e regulamentações com a finalidade de viabilizar as novas formas eletrônicas de interação do governo com o cidadão (G2C), com outros governos (G2G) e com seus fornecedores (G2B).

Em junho de 2000, foi publicada a Política de Segurança da Informação, através do Decreto Nº 3.505. Em setembro do mesmo ano foram estabelecidas normas para a ICP-Gov, através do Decreto Nº 3.587 e apresentada uma proposta de políticas de governo eletrônico para o Poder Executivo. Em outubro, foi criado o Comitê Executivo de Governo Eletrônico (CEGE), através do Decreto de 18 de outubro de 2000, que tinha por objetivo formular políticas, estabelecer diretrizes, coordenar e articular as ações de implantação do Governo Eletrônico.

Em janeiro de 2001, foi a regulamentação legal e normativa para o uso de documentos eletrônicos na Administração Federal. Em junho, foi criada a ICP-Brasil, através da Medida Provisória Nº 2.200, com a finalidade de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, assim como a

realização de transações eletrônicas seguras. Em outubro foram estabelecidas as primeiras diretrizes sobre a prestação de serviços de certificação digital.

Em 2003, o ITI passa a ser vinculado a Casa Civil da Presidência da República.

> Desde janeiro de 2001, a Presidência da República passou a receber documentos dos Ministérios, exclusivamente em meio eletrônico, com uso da certificação digital. Foi implantada a expansão da tramitação eletrônica de documentos, envolvendo os Gabinetes de Ministro e as Secretarias de Ministério, por meio do Sistema de Geração e Tramitação de Documentos Oficiais – SIDOF. E, somente a partir de 17 de dezembro, a divulgação dos atos oficiais federais pelo sítio da Imprensa Nacional na internet passou a ser realizada *on-line*, tão logo assinado e numerado o documento e autorizada sua publicação (IGTI, 2014)

Em 31 de maio de 2004, foi publicado o documento de referência sobre os Padrões de Interoperabilidade em Governo Eletrônico (e-PING), que dentre outras questões, estabelece que o uso de criptografia e certificação digital, para a proteção do tráfego, armazenamento de dados, controle de acesso, assinatura digital e assinatura de código, deve estar em conformidade com as regras da ICP-Brasil.

O Termo de Referência do Comitê Gestor ICP-Brasil surgiu da necessidade de definição de um arcabouço de normatização institucional que detalhasse as suas funções, atribuições, competências e organização funcional, onde foram definidos nove princípios básicos, que devem ser satisfeitos, a fim de garantir a eficácia da ICP-Brasil:

1) *Responsabilização* – a responsabilidade e a responsabilização dos proprietários, prestadores de serviço e usuários de sistemas de informação e outras partes envolvidas com a segurança dos sistemas de informação devem ser explicitas e documentadas;

2) *Conhecimento* - os proprietários, prestadores de serviço e usuários dos sistemas de informação e outras partes envolvidas devem prontamente, e de maneira consistente com a manutenção da segurança, adquirir conhecimentos apropriados da existência e da abrangência geral das medidas, práticas e procedimentos relacionados à segurança dos sistemas de informação, mantendo-se informados sobre esse conjunto normativo;

3) *Ética* – os sistemas de informação que integrarão a ICP-Brasil e os seus mecanismos de segurança deverão ser fornecidos e utilizados de maneira tal que os direitos e interesses legítimos de outrem sejam respeitados;

4) *Multidisciplinaridade* - normas, práticas e procedimentos relacionados com a segurança dos sistemas de informação integrantes da ICP-Brasil deverão considerar os pontos de vista relevantes, inclusive os técnicos, administrativos, organizacionais, operacionais, comerciais, educacionais e jurídicos, tratando cada um destes de forma adequada;

5) *Proporcionalidade* - A ICP-Brasil deverá contemplar níveis de segurança, normas, práticas e procedimentos compatíveis com a criticidade, a importância e o valor dos sistemas de informação que a utilizem, considerando-se os ambientes específicos envolvidos;

6) *Integração* - as normas, práticas e procedimentos relacionados à segurança dos sistemas de informação deverão ser coordenados e integrados de modo a se criar um conjunto harmônico e coerente de segurança da informação para o governo e sociedade civil;

7) *Atualização* - a segurança dos sistemas de informação integrantes da ICP-Brasil deverá ser reavaliada periodicamente, na medida em que os sistemas de informação e as exigências ligadas à sua segurança variam em relação ao tempo e momento tecnológico considerado;

8) *Escalabilidade* - a perspectiva de crescimento que abrange tanto o número de aplicações quanto à quantidade de usuários; e

9) *Interoperabilidade* - os sistemas que compõem a ICP-Brasil preferencialmente devem obedecer ao paradigma de sistemas abertos de modo a se reduzir ao máximo as incertezas relacionadas com a integração de outros sistemas à infraestrutura existente.

### 2.3.4 Panorama de publicações sobre Certificação Digital no Brasil

Foi realizada uma busca sistemática da literatura em bases de dados nacionais e internacionais onde foi feito um levantamento de artigos, dissertações e teses referentes à certificação digital no Brasil, a fim de entender como este tema está sendo abordado no Brasil e quais os maiores focos de pesquisa.

As bases de dados escolhidas foram as bases Scopus, SciELO e Portal da CAPES, bem como a Biblioteca Nacional Brasileira de Teses e Dissertações da IBICT, Sistema Integrado de Bibliotecas da

Universidade de São Paulo – SibiNet e o Sistema de Biblioteca da UFSC. Como complementação das buscas, recorreu-se ao Google Acadêmico na busca de artigos nacionais publicados em eventos ou em revistas não indexadas, e de teses e dissertações que por ventura não tenham sido encontrados nos Bancos de Teses e Dissertações - BTDs mencionados.

A seleção das palavras-chave utilizadas no processo de busca foi determinada mediante a relevância das mesmas ao propósito desta pesquisa, sendo elas: 1) certificação digital; 2) certificado digital; 3) infraestrutura de chaves públicas; 4) ICP-Brasil; 5) assinatura digital[2]

O processo de busca nas bases de dados obedeceu aos seguintes critérios e delimitações:

- Para a busca das palavras-chave foram consideradas as palavras exatas;
- Recorreu-se ao operador lógico "OR" para combinação das palavras-chave utilizadas para rastreamento das publicações;
- Limitou-se a busca por publicações no âmbito do Brasil;
- No Portal da CAPES limitou-se a busca por periódicos revisados por pares;
- Na base de dados Scopus limitou-se a busca por artigos que contivessem estritamente em seu título uma das variáveis.

A busca compreendeu o período de 1999 a setembro de 2014 e resultou em 27 artigos e 74 teses/dissertações, que foram analisados e classificados de acordo com o foco principal, abordado em cada uma delas.

Após as primeiras apreciações resultantes da busca sistemática, foram selecionadas para análise as publicações cujo foco principal era a certificação digital, o que resultou na análise integral de 13 artigos e 30 dissertações e teses, ou seja, 43 publicações.

As publicações analisadas na íntegra foram agrupadas de acordo com o foco da pesquisa, em quatro categorias: (i) **total aderência ao tema certificação digital no que concerne a aspectos teóricos** (totalizando 11 publicações); (ii) **impacto do uso da certificação digital no Brasil**(totalizando 4 publicações); (iii) aplicações da certificação digital (totalizando 23 publicações) e (iv) trabalhos cujo teor

[2] Na base de dados Scopus a busca foi realizada a partir das palavras-chave em inglês (*digital certification*; *digital certificate*; *Public Key Infrastructure*; *digital signature*)

fazem uma análise crítica da ICP-Brasil: dos normativos e jurídicos aos aspectos técnicos (totalizando 5 publicações)

#### 2.3.4.1Publicações com enfoque teórico sobre a certificação digital no Brasil

Esta seção tem por objetivo apresentar sucintamente as publicações que focaram aspectos gerais da certificação digital, seja realizando um histórico da ICP-Brasil, seja definindo a certificação digital, seus aspectos tecnológicos ou fazendo uma comparação entre ICP-Brasil e ICPs de outros países.

Dos trabalhos analisados que enfocam estes aspectos, somaram 11 publicações, sendo 6 artigos e 5 dissertações, sendo eles:

Koerich (2012) em seu artigo intitulado "**Sustentabilidade da Infraestrutura de Chaves Públicas Brasileira**", desenvolve um modelo (econômico-financeiro), a partir de uma abordagem teórico-empírica, que permita avaliar em diferentes cenários a estrutura operacional adequada para o funcionamento das entidades emissoras de certificados digitais em longo prazo. Explica os custos de AC e AR e ainda as receitas, faz uma análise de cenários, comparando o valor atual e um pequeno aumento que garante a sustentabilidade do sistema.

Sutil (2011) (dissertação intitulada "**Gestão segura de múltiplas instâncias de uma mesma chave de assinatura em autoridades certificadoras**"), buscou tratar o problema da gestão de chaves criptográficas sob uma ótica que se preocupe com o controle das múltiplas instâncias de uma mesma chave, ao longo de sua vida útil, buscando sempre mantê-las sob o controle dos custodiantes. O modelo buscou ainda tornar evidente o procedimento de backup ou replicação, por intermédio de um rastro, amarrando a chave original às suas réplicas, que permita um processo de auditoria mais simples e com menor custo, bem como a identificação das diferentes instâncias. Este trabalho trouxe como contribuições os principais estados necessários à gestão segura do ciclo de vida de chaves criptográficas. Assim, no que se refere à garantia de proteção, o modelo agrega além da confiabilidade, autenticidade, não repúdio e integridade, requisitos como: disponibilidade (as chaves devem estar disponíveis sempre que requisitadas por aqueles que têm direito de acesso); controle sobre acesso (acesso seja feito somente por entidades devidamente credenciadas e autorizadas); registro de utilização (controle de uso das chaves deve ser devidamente garantido de forma a permitir a

identificação precisa de cada momento em que o artefato foi utilizado, destruído, copiado etc.); rastreabilidade (como forma de garantir sua disponibilidade, cópias da chave devem ser distribuídas em locais distintos, com segurança controlada, sendo necessário garantir que estas cópias sejam devidamente registradas e possam ser rastreadas sempre que necessário); unicidade (garantia de que a chave seja única, estando sempre sob o controle de seu titular); tempestividade (chaves criptográficas, bem como os algoritmos a que se destinam, têm um tempo de vida finito, onde precisarão ser substituídos por outras soluções ou, no caso das chaves, por versões mais fortes, ou seja, sempre que seu nível de proteção torne-se inadequado). Sob a ótica da segurança, descreve quatro níveis: que variam da proteção não física, restrições de acesso através de segurança física, autenticação dos operadores autorizados e a introdução de mecanismos de resposta a ataques, à segurança física rígida.

Kohler (2011) (dissertação intitulada "**Análise de políticas na integração de infraestruturas de chaves públicas**"), buscou analisar e propor mecanismos que permitam a integração de ICPs considerando domínios de certificação embarcados em dispositivos. Os resultados desse estudo permitiram gerar inúmeros mecanismos e formas diferentes de realizar a integração entre duas ICPs. Dentre diversas simulações de integração, foram realizadas simulações integrando a ICP Portuguesa e a ICP-Brasil. Os resultados encontrados nestas simulações foram caracterizados como muito bons; no entanto, alguns aspectos ainda não foram totalmente resolvidos.

Costa (2010) (dissertação intitulada "**Modernização dos processos de auditoria e fiscalização da ICP Brasil**"), propôs um modelo para modernizar os processos de auditoria e fiscalização da ICP-Brasil, por meio da automação e do uso do documento eletrônico seguro. A justificativa do autor para a proposição do modelo é que muitos processos da ICP-Brasil ainda são feitos de forma manual e com o suporte do documento em papel. Desta forma, modelou os processos de auditoria e fiscalização de forma a automatizá-los por meio do uso de certificação digital. O modelo automatizado permite que a AC Raiz controle o fluxo de informação do processo de auditoria. Conclui que o modelo proposto é viável e possível de ser implementado, mas necessita de estudos aprofundados.

Resende (2009) (artigo intitulado "**Certificação Digital**"), aborda massivamente os aspectos teóricos da certificação digital. Observa que o recurso chamado de Assinatura Digital é muito usado com chaves públicas, como se fosse um "reconhecimento de firma digital".

Diferencia assinatura digital e criptografia; a primeira serve para provar a autenticidade e origem dos dados em uma mensagem ou documento; a segunda é utilizada para privacidade. Muitas operações bancárias e transações só se tornam válidas legalmente depois de serem assinados digitalmente seus documentos. Do ponto de vista jurídico, as consequências jurídicas, propriamente ditas no tocante à certificação eletrônica, a responsabilidade maior dever ser da certificadora. Em casos de descumprimento das normas atribuídas à certificadora, esta pode ser descredenciada. O que traria grande insegurança jurídica, pois todos os documentos assinados digitalmente, oriundos daquela credenciadora estariam sob suspeita. Até mesmo o ITI, como órgão superior, em razão de ter suas atividades aprovadas pelo Comitê Gestor, também está sujeito à fiscalização e à descredenciamento. É notório que as fraudes podem ocorrer tanto no mundo físico quanto no digital, e esse problema é inerente ao ser humano, e tem a ver com a ética e a moral de cada um. Não cabe à informática interferir, mas através dela, se todos os cuidados forem tomados, o trabalho se torna mais fácil. Cabe lembrar que a falsificação de uma certidão digital tem as mesmas consequências jurídicas que a falsificação de uma certidão de papel. Buscou ainda analisar o impacto da certificação digital no que se refere à segurança da informação e obteve como resultado uma gama de benefícios em que a certificação digital proporciona: agilidade nos processos burocráticos, redução de custos, prove maior segurança nas transações pela internet, respaldo legal e sigilo nas negociações; cita alguns exemplos dessas vantagens. Conclui que o Governo é um dos grandes incentivadores do uso do certificado digital e que outra grande vantagem a ser pensada é que o impacto ambiental é preservado, devido a imensa economia de papel.

Quaquio (2009) (artigo intitulado "**Infraestrutura de Chave Pública (ICP)**", descreve a Infraestrutura de Chave Pública usando certificados digitais baseados em chave pública e o que é a ICP-Brasil, além de como e quando usar certificado digital e descreve um possível futuro da tecnologia. Conclui que as transações e os negócios on-line estão cada vez mais presentes em nossas vidas, onde o consequente crescimento, a redução de custos e a versatilidade dessa "identidade virtual" chamada Certificado Digital, com certeza, será o método mais utilizado para garantir a confidencialidade, a integridade e o não-repúdio dos dados trafegados pela Internet.

Freitas e Veronese (2007) (artigo intitulado "**Segredo e Democracia: certificação digital e software livre**", em um primeiro momento, tratam da criptografia no panorama internacional: do segredo

de Estado à garantia de comunicação livre. Posteriormente, apresentam a formação do Instituto e a construção de agenda política de certificação digital. Concluem que o segredo gerado pelo uso da certificação digital não ataca os princípios democráticos que regem as sociedades contemporâneas, já que a confidencialidade a ela associada diz respeito ao direito do indivíduo (ou grupo) de exercer sua liberdade civil (individual ou coletiva). As noções de democracia e segredo entrelaçam-se e não se contrapõem, isto é, a noção de segredo e a de democracia apresenta-se de forma complementar e não dicotômica, se geridas em uma pauta comum.

Barra (2006) (dissertação intitulada "**Infraestrutura de chaves públicas brasileira (ICP-Brasil) e a formação do estado eletrônico**"), buscou compreender o que possibilitou o surgimento da chamada ICP-Brasil. Concluiu que os bancos proporcionaram a precondição socioeconômica para a instituição da ICP-Brasil, mas que estiveram fora dos processos que transcorreram no Poder Executivo. A precondição socioeconômica proporcionada pelo apoio dos bancos à ICP-Brasil relacionou-se diretamente ao interesse político de incorporar um ator de peso na economia que garantisse o uso da infraestrutura, além do uso que faria a própria máquina do Estado. Em suma, a ICP-Brasil foi instituída como resultado de um processo político, cuja condição sociopolítica, enquanto Razão de Estado influenciou mais o processo do que os próprios políticos governantes, evidenciando a questão como eminentemente de Estado. A superação da situação de Razão de Estado colocada pela ICP-Brasil envolveu esforço conjunto de atores de três grupos sociais: políticos do executivo, burocracia do Estado e segmento bancário que, reunidos por meio de uma política de alianças, utilizaram seus recursos de poder. A ICP-Brasil, em sua construção, associou-se à análise e compreensão da situação internacional, assim como a negociação política na esfera internacional, visando à adoção de uma opção tecnológica.

Lins (2005) (artigo intitulado "**Comércio eletrônico, assinatura e certificação digital**"), descreve a tecnologia de criptografia, a assinatura digital, alguns aspectos da estrutura de certificação, a implementação da ICP-Brasil e algumas aplicações da assinatura digital e possíveis oportunidades de ação legislativa. Em relação a criptografia simétrica, ela permite que grandes arquivos sejam criptografados e descriptografados rapidamente, mas o processo de transferência da chave do remetente não é seguro, uma vez que ela pode ser conhecida por mais de uma pessoa ou máquina, não servindo para comprovação de autoria. Na criptografia assimétrica, se as chaves forem suficientemente

grandes, é impossível, ou muito difícil, a dedução de uma das chaves a partir da outra, mas tem como desvantagem a lentidão no processo de criptografia, o que pode ser resolvido com a criação de um registro auxiliar: código *hash* ou registro de *hash*. Este mecanismo atende aos critérios de aceitabilidade como meio de prova. Coloca que a garantia da revogação do certificado é um mecanismo que tem riscos, pois pode decorrer um período entre a quebra da segurança da chave e a descoberta dessa quebra e que as AC's devem gozar da confiança pública e implementar procedimentos seguros de atendimento. Descreve o processo de datação com carimbo de tempo.

Menke (2003) (artigo intitulado "**Assinaturas Digitais, Certificados Digitais, Infraestrutura de Chaves Públicas Brasileiras e a ICP Alemã**") traz uma contribuição teórica do modelo de ICP brasileiro, a partir de uma análise comparativa com o modelo alemão de ICP, na qual a concepção do modelo brasileiro se espelhou. Apresenta um histórico do modelo de ICP-Alemã, cujo modelo é caracterizado por ser uma ICP de base nacional com a presença de uma entidade pública na posição de supervisão do sistema. Afirma que na Europa o modelo alemão é o mais desenvolvido e que as vantagens de uma ICP nacional com a presença de uma entidade pública na posição de supervisão do sistema são inúmeras, e apresenta. Como contraexemplo desse fato, que o modelo americano de ICP – ao não adotar uma ICP nacional com a presença de uma entidade pública na posição de supervisão – se desenvolveu de forma desorganizada, com diversas ICPs tanto em iniciativas governamentais quanto em iniciativas privadas. Desta forma, conclui que o Brasil seguiu o caminho mais adequado ao optar por um modelo de ICP que tenha no ápice da cadeia de certificação uma entidade de direito público com a finalidade de credenciar e fiscalizar as operações das Autoridades Certificadoras, que tencionem obter os níveis mais altos de segurança em suas operações.

Parra (2002) (dissertação intitulada "**Metodologia para Análise de Segurança Aplicada em uma Infraestrutura de Chave Pública**"), propõe uma metodologia simplificada para auxiliar empresas que emitem certificados digitais para analisar a situação atual de segurança. A Metodologia Simplificada para Análise de Segurança – MAS, apresentada, foi desenvolvida para possibilitar que organizações como as ICPs tenham conhecimento e saibam exatamente quais os aspectos de segurança que deverão ser tratados com prioridade. Apesar dessa metodologia ser focada para organizações ICP, também pode ser aplicada para organizações com contexto semelhante.

2.3.4.2 Publicações com enfoque nas aplicações da certificação digital no Brasil

Esta seção tem por objetivo apresentar sucintamente as publicações que abordaram as aplicações da certificação digital, que totalizou 23 publicações, que foram divididas para esta análise em seis grupos de assuntos: Documentos Eletrônicos (totalizando 5 publicações); Contratos Eletrônicos (totalizando 3 publicações); Cartórios Brasileiros (totalizando 2 publicações); Justiça Brasileira (totalizando 6 publicações); Saúde (totalizando 4 publicações); e outras aplicações (totalizando 3 publicações).

**Documentos Eletrônicos**

Leal (2013) (dissertação intitulada "**O documento eletrônico seguro nas transações de compras eletrônicas**"), analisou a adoção do Documento Eletrônico Seguro (DES), via certificação digital ICP-Brasil, por parte de organizações usuárias de um portal de compras eletrônicas, através de entrevistas estruturadas, por meio de um questionário eletrônico, com 18 organizações usuárias de um portal de compras eletrônicas. O estudo mostrou que a adesão ao documento eletrônico seguro ainda é muito discreto nas organizações pesquisadas, embora ressalte que ainda tem uma demanda reprimida por assinatura digital, uma vez que os documentos gerados no portal de compras são todos eletrônicos, não existindo a necessidade de sua impressão para assinatura manual. Os **benefícios** citados pelos entrevistados com a utilização de documentos eletrônicos foram: redução significativa de custos e despesas com papel, com tempo, com transporte e com armazenamento em arquivos físicos. Contudo, a forma predominante nas transações das compras eletrônicas do referido portal é por meio de usuário e senha. Como impactos na organização para a adoção do DES o destaque foi para os custos com aquisição e evolução dos sistemas informatizados; a alteração no fluxo dos processos de compras; a melhoria na eficiência do processo de compras; a resistência dos usuários às mudanças. Apresenta ainda as maiores **barreiras** enfrentadas para o uso do documento eletrônico seguro que, segundo as organizações pesquisadas, são o custo com a aquisição ou ajuste dos sistemas informatizados e principalmente o custo do certificado digital.

Vigil (2010) (dissertação intitulada "**Infraestrutura de Chaves Públicas Otimizadora", propôs uma "Infraestrutura de chaves públicas otimizadora**", a implementação de um novo conceito de certificado: o Certificado Otimizado, base da Infraestrutura de Chaves Públicas Otimizadora. Em outras palavras, o certificado otimizado é uma abordagem para facilitar a verificação e a manutenção a longo prazo da autenticidade de documentos assinados. Trata-se de adaptações ao padrão X.509 para reduzir o esforço computacional necessário ao uso de documentos eletrônicos assinados sem a perda da compatibilidade com as aplicações existentes. Tal redução incide na verificação de assinaturas digitais, pois o Certificado Otimizado: (1) dispensa verificação de situação de revogação; (2) substitui carimbos do tempo sobre uma assinatura digital; (3) é emitido por uma autoridade certificadora cuja situação de revogação é aferida através do método "Novo modo"; e (4) possui um caminho de certificação curto. Esta proposta também explora a substituição de certificados otimizados quando da obsolescência dos algoritmos criptográficos, tornando possível a manutenção da autenticidade de assinaturas digitais sem o aumento contínuo dos recursos computacionais utilizados. Além disso, a solução é comparada com o certificado X.509 convencional através da simulação de um cenário de documentos eletrônicos assinados na ICP-Brasil. Concluiu que a abordagem utilizada visa reduzir e manter constante o volume de dados de validação para assinaturas digitais sobre documentos eletrônicos.

Tuci e Laurindo (2006) (artigo intitulado "**O Impacto da Certificação Digital na Operação de Comercialização de Seguros**"), realizaram um estudo a fim de mostrar que a eliminação dos documentos físicos e o uso da certificação digital tende a trazer algumas vantagens para os processos de operacionalização de comercialização de seguros. Por meio de uma pesquisa de campo realizada com 15 representantes das companhias de seguro, foi verificado quais os processos seriam beneficiados com a implantação da certificação digital e quais seriam os benefícios diretos ocasionados pela implantação da nova tecnologia. Os dados obtidos foram que os **benefícios com relação a processos operacionais que envolvem o segurado/participante** foram: Aumento das alternativas de escolha; Informações detalhadas sobre os produtos e possibilidade de contratação imediata; Disponibilidade de serviços on-line; Conveniência e disponibilidade 24h (onde quer que o segurado/participante se encontre); e Redução do tempo total das transações.**Com relação a processos operacionais que envolvem as companhias** foram: Aumento da probabilidade da venda

direta; Redução da burocracia na comercialização; Velocidade na contratação; Segurança da identidade dos contratantes e contratados; Garantia de integridade dos documentos eletrônicos e menores custos com a movimentação de papel; Redução de tempo de entrega com garantia de recebimento e reconhecimento; e Redução do trâmite processual dentro da companhia.**Com relação a processos operacionais que envolvem os corretores/ parceiros/ canais** foram: Redução dos custos das propostas, sobretudo para os casos de seguros de baixo valor; Maior variedade nos produtos ofertados para os clientes; Ciclo de contratação reduzido; Maior agilidade e facilidade no fornecimento de informações; Maior integração com as seguradoras e com seus clientes corporativos; Personalização e possibilidade reais de vendas cruzadas; Aumento da capacidade de atendimento; Economia de tempo, por meio da otimização de processos internos das empresas; e Redução da fraude no setor, eliminando do fluxo de papéis e valores durante o processo de contratação. Desta forma, concluíram que a implantação efetiva da certificação digital ICP-Brasil propiciará uma evolução da indústria de seguros que, por sua vez, esta evolução permitirá a redução de custos das propostas comerciais, economia de tempo e papel, redução de fraudes nas operações, agilidade nas contratações, maior capacidade de atendimento, aumento da integração entre as seguradoras e clientes via web, maior oferta de produtos e serviços e ganho de escala nos diversos processos de negócio.

Kazienko (2003) (dissertação intitulada "**Assinatura Digital de Documentos Eletrônicos Através da Impressão Digital**", aborda a utilização da impressão digital como meio de verificação da identidade do usuário quando da assinatura digital de documento eletrônico, onde aplica um modelo desenvolvido para o registro de ocorrências policiais da Polícia Civil do estado de Santa Catarina, denominado Boletim de Ocorrência Eletrônico Seguro – BOES, que é a proposta de um sistema voltado para o registro de ocorrências policiais pela Internet, viabilizado por meio de assinatura e certificado digital para autenticação das informações prestadas. Os aspectos fundamentais em relação ao BOES são: universalização dos registros de BOs, segurança da informação e popularização do uso de BOs. Conclui que o sistema proposto contribui para a melhoria no processo de registro de ocorrências policiais de acordo com os seguintes itens: agilidade nos processos; custo reduzido e ênfase a investigação; formas de acesso e segurança; aumento na notificação de crimes e; rastreabilidade de ocorrência de delitos.

Minella (2002) (dissertação intitulada "**Sistema de disponibilização de documentos legais de forma eletrônica**",

apresenta um sistema de disponibilização de documentos legais de forma eletrônica, denominado Sistema de Disponibilização de Documentos Legais de forma Eletrônica (SDDL), que venha desburocratizar o acesso do público em geral à documentação de sua propriedade, em órgãos disponibilizadores como prefeituras, cartórios e órgãos públicos, de forma rápida, segura e confiável, sem dependência de horário de atendimento e deslocamento físico, utilizando a Internet como meio de acesso ao sistema, contando com apoio de tecnologias recentes de segurança e apoiando-se em leis que regem a validade de assinatura digital e de documentos eletrônicos. O uso do recurso de identidade digital, se faz necessário para controle da obtenção e autenticação dos documentos, visando adequar o sistema a normas regidas por leis que dão validade e autenticidade a documentos eletrônicos. O sistema desenvolvido se utiliza de formas atuais de acesso ao sistema e autenticação de documentos eletrônicos usando certificados digitais, mas mantém também formas próximas à tradicionais para acesso e autenticação, a fim de popularizar seu uso. Conclui que em relação ao método tradicional existente de disponibilização de documentos autenticados, o SDDL tem grande vantagem no que se refere a encurtar distâncias e tempo na obtenção de tais documentos; obviamente, desde que não haja atrasos por parte das Órgãos Disponibilizadores de Documentos (ODDs). Onde, quanto maior for a integração entre as ODDs maior será o contingente de informações disponibilizadas e integradas e maiores seriam as vantagens de uso e interesse do usuário de se adequar à esta nova tecnologia. Por fim, salienta-se que propostas desta natureza envolvem muitos aspectos legais e sua implementação dependeria do aval de órgãos públicos competentes. Além disso, entraves na popularização do uso de tais recursos devem ser vencidos com a utilização de métodos e políticas de incentivo ao uso. Pois, de nada adianta a implantação de tecnologias avançadas, sem que o principal componente, o usuário, se beneficie e gere receita que viabilize a continuidade e modernização dos recursos oferecidos.

**Contratos Eletrônicos**

Cesaro e Rabello (2012) (artigo intitulado "**Um modelo para a implementação de contratos eletrônicos válidos**"), apresentam um modelo de implementação para um módulo de geração de contratos eletrônicos válidos, buscando na atual legislação, um enquadramento

para a contração eletrônica. Tal modelo tem como premissa básica a conformidade com os requisitos técnico-legais, tais como preservação de provas e mitigação de riscos relacionados à violação dos diretos autorais, de integridade e de repúdio. O modelo resulta em um protótipo para geração de contratos eletrônicos válidos, onde a declaração da vontade é realizada através da biometria por impressão digital. Respeitando o direito de imagem e privacidade, o indivíduo deve concordar com o fornecimento dos dados biométricos pela aceitação de um termo. Para garantir a integridade do documento eletrônico, o modelo utiliza-se da certificação digital e para comprovar o exato momento de celebração do processo, o modelo utiliza o carimbo do tempo. Os autores concluem que contratos comerciais ou de prestação de serviço, firmados no meio eletrônico, têm validade legal, desde que seja possível comprovar a manifestação da vontade das partes, isto é, da prova de autoria e integridade do documento eletrônico. Nesse sentido, o modelo de implementação exemplifica a utilização de recursos computacionais necessários para atender às exigências da lei e demonstrar a sua viabilidade técnica através de um protótipo.

Behrens (2005) (dissertação intitulada "**A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira**"), levanta a relevância da assinatura digital, consolidada pelo instrumento da certificação digital, por uma autoridade certificadora, seja ela pública ou privada, como meio de validar os instrumentos digitais de contratos eletrônicos. Com a implementação da ICP-Brasil, instituída pela MP 2.200, um corpo de normas e políticas tem respaldado para que as relações jurídicas sejam adequadamente tuteladas. Contudo, o autor levanta a problemática de que como esses novos métodos são incipientes, nem sempre são completamente protegidos pela legislação que encontra extrema dificuldade em se manter atualizada em face às novas tecnologias, e que merece uma atenção especial de juristas e legisladores. Além disso, traz à tona a questão da inclusão digital, pois a migração de um processo físico à eletrônico não pode torna-se excludente.

Barbagalo (2000) (dissertação intitulada "**Contratos eletrônicos: contratos formados por meio de redes de computadores peculiaridades**"), coloca que a identificação quanto às partes nos contratos eletrônicos é um fator que merece grande atenção. Já nessa época, nos anos 2000, o autor enaltece a existência de tecnologia que garante a autenticidade das partes por meio de assinatura digital que, por sua vez assegura, além da procedência da declaração de vontade, também sua integridade. Desta forma, para maior segurança, sugere-se a

utilização de certificados digitais concedidos por autoridade certificadora, a qual atua como terceiro garantidor da identidade da pessoa para quem o certificado digital é criado.

**Cartórios Brasileiros**

Pereira (2011), (dissertação intitulada "**Protocolo para emissão de Assinatura Digital utilizando compartilhamento de segredo**"), evidencia a eficácia da assinatura digital, possibilitada via certificação digital, em serviços disponibilizados por organizações como Cartório. Afirmando que o uso de assinatura digital para o processo de reconhecimento de firma por semelhança é mais seguro que o processo de reconhecimento de firma por similaridade, uma vez que a prova de autoria e irretratabilidade da assinatura digital é feita por meio por meio de fundamentos matemáticos, diferentemente do processo convencional em que a comparação das assinaturas é feita por um funcionário, sendo que este pode estar despreparado ou sem a devida atenção, colocando em risco todo o processo de reconhecimento de firma. Contudo, no caso de reconhecimento de firma por autenticidade, a implementação da assinatura digital neste processo não é uma tarefa tão simples, existe um grau de complexidade maior que permeia este serviço no meio digital. Essa complexidade se deve ao fato que o reconhecimento de firma por autenticidade exige a presença física do signatário como requisito para elevar o nível de segurança e certeza de reconhecimento. A certificação digital até garante a autoria da assinatura digital, mas não garante que o documento assinado digitalmente foi assinado pelo dono da assinatura, pois o certificado digital é armazenado em algum dispositivo (Token; cartão de memória) e este, por sua vez, pode ser furtado ou corrompido, ocorrendo isto, não se pode afirmar que há autenticidade da assinatura digital do documento. A fim de eliminar esse gargalo, propôs um protocolo para emissão da assinatura digital por autenticidade. Para desenvolver o protocolo utiliza como exemplo, o processo de reconhecimento de firma por autenticidade, mas ressalta que o protocolo desenvolvido pode ser utilizado para outros contextos. No protocolo proposto, o compartilhamento de segredos é utilizado para se dividir responsabilidade da garantia de autenticidade do documento e da assinatura dos usuários. O que significa que, para garantir a segurança da assinatura digital do usuário, ela deve ser dividida em partes e suas partes armazenadas em locais distintos, isto é, a chave privada não deve

ser armazenada em um único dispositivo. Assim, somente uma parte da chave privada é armazenada no dispositivo do usuário. A outra parte pode, por exemplo, ficar sob responsabilidade dos cartórios, já que estes são órgão públicos que reconhecem firmas e autenticam documentos; sendo assim, devem também ter sua parcela de responsabilidade na emissão de uma assinatura digital, por autenticidade, e no armazenamento da chave privada. Na prática o processo se estabelece da seguinte forma: o cartório reconhece a firma do computador e do vendedor em um documento, sendo, portanto, uma testemunha de que as assinaturas no documento são válidas. Assim, se vários elementos, cartório, vendedor e comprador, participarem da emissão da assinatura em um documento, eles reconhecerão a firma e o documento como autênticos, pois eles ajudaram a emitir a assinatura se tornando testemunhas. Onde para garantir o sigilo das informações transmitidas, foi empregado o esquema de criptografia do RSA, por considerar ser um dos mais usados atualmente e também por ser pelo ITI, responsável pela ICP-Brasil. Coloca que a utilização da certificação digital por organizações como os cartórios, não só facilita as suas atividades tornando-as mais ágeis e seguras como também transmite a população brasileira o sentimento de confiança nessa nova tecnologia. Acrescenta ainda que a certificação digital é bastante útil as autenticações digitais oferecidas e auxilia no tráfego das informações.

Bortoli (2002) (dissertação intitulada "**O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais**"), propôs mostrar a viabilidade dos cartórios adotarem o uso do documento eletrônico na emissão e armazenamento dos registros e documentos em geral. Partiu, primeiramente, no desenvolvimento de um protótipo para a Emissão de Registros Públicos pela internet, especificamente da Emissão de Registro de Nascimento, em parceria com a Maternidade do Hospital Universitário da UFSC, onde o Laboratório de Segurança em Computação – LabSec em cooperação com o Laboratório de Informática Jurídica, ambos da Universidade Federal de Santa Catarina (UFSC), desenvolveram um projeto denominado Cartório Virtual cujo objetivo é promover os serviços dos cartórios convencionais via internet. Esse cartório está organizado na forma de diversos projetos. Esse protótipo resume-se aos seguintes processos: com o uso da tecnologia de assinatura digital, o cartório (devidamente credenciado pela Autoridade Certificadora da UFSC) poderá autorizar o funcionamento do Cartório Virtual ao estabelecimento, que neste caso é a Maternidade do Hospital Universitário da UFSC, este por sua vez, poderá acessar o sistema de Cartório Virtual da Web, por meio de um agente autorizado e certificado

por Autoridade Certificadora, que colocará no sistema as informações de nascimento, com os dados correspondentes à Declaração de Nascido Vivo – DN e mais os dados necessárias à efetivação do registro de nascimento. Com base nesse protótipo algumas considerações, no sentido de ampliar a proposta foram feitas, por exemplo, a extensão dos processos do protótipo de registro de nascimento aos registros de casamento e óbito, em função da ligação que existe entre esses registros civis. Desta forma, quando o indivíduo sofre qualquer alteração em sua situação civil, a base de dados do cartório recebe estas informações automaticamente. Acrescenta que no processo virtual os documentos do cartório ficariam armazenados na base dados do Cartório Virtual, e todos os cartórios, desde que habilitados a operarem virtualmente as informações, poderiam automaticamente acrescentar dados aos registros. Com relação a perda de informações, para evitar esses riscos, caso o cartório venha a perder a sua chave privada, foi proposto que o lacre de informações fosse compartilhado com outra entidade, diretamente ligada ao Poder Judiciário, por meio da aplicação da cifragem com a chave pública do cartório e do cliente. Conclui que o cartório do futuro passará por um longo período de transição em que o documento eletrônico irá substituindo lentamente o documento de papel. Não acredita que o documento de papel seja substituído completamente, pois apesar dos avanços tecnológicos, especialmente na área de segurança das informações que transitam pela rede, ainda assim há muitas dúvidas em relação às garantias da integridade do documento eletrônico, e sua eficácia em substituir os documentos de papel por completo.

**Justiça Brasileira**

Merino Recinos (2012) (dissertação intitulada "**A importância do processo eletrônico, enquanto mecanismo célere de acesso à justiça, e diagnóstico de sua viabilidade em El Salvador**"), contextualizou o surgimento da informatização do processo com base na lei 11.419/06 que institui o encaminhamento de autos processuais assinados eletronicamente mediante o uso de certificados digitais vinculados à ICP-Brasil, para logo, formular-se, a partir da experiência brasileira, um diagnóstico situacional de processo eletrônico para El Salvador.

Martinez et al. (2012) (artigo intitulado "**A Assinatura Digital e o Processo Judicial Eletrônico: Um Estudo do Impacto da**

**Revogação do Certificado Digital na Validade dos Atos Processuais**"), apresentam conceitos a respeito de temas envolvidos com a certificação digital, dando ênfase às atividades que este certificado proporciona e multiplicando informações diversas sobre um tema ainda considerado novo para muitos empresários e estudantes. Utiliza uma ideia interessante da ICP como um "cartório virtual". Citam a tendência do crescimento de uso da certificação e conclui que o Brasil está preparado, até mesmo estruturalmente, para funcionamento da certificação e passou a criar meios de obrigatoriedade do uso. Com base nas consultas realizadas pelos pesquisadores, foram analisados os impactos da revogação do certificado digital na validade dos documentos eletrônicos, por meio dos quais os atos judiciais são praticados, considerando a adoção da assinatura digital no processo judicial eletrônico. A sentença é gerada digitalmente e assinada com um certificado emitido dentro da estrutura da ICP-Brasil. Proferida a decisão, que é registrada no sistema, a sentença é assinada digitalmente na própria audiência. No momento da publicação, qualquer interessado tem acesso imediato, via internet, ao inteiro teor da sentença. O sistema tem tido plena aceitação por parte de magistrados, servidores, advogados e partes. Todavia, uma das diferenças entre a assinatura em papel e a assinatura digital reside no fato de que o certificado digital pode ser revogado. A revogação do certificado digital pode ocorrer por conta do usuário, quando "a chave é comprometida" ou "alguma informação do certificado é alterada", ou por conta de alteração no processo de assinatura, ou seja, se a data da assinatura encontra-se dentro do período de uso permitido, a assinatura é considerada válida. Se a data da assinatura encontra-se dentro do período de validade do certificado, mas fora do período de uso permitido, a assinatura é considerada inválida. Concluem que um dos problemas que se apresentam em relação à adoção dos certificados digitais envolve a validade do certificado, no momento da assinatura digital. Os métodos e técnicas forenses permitem investigar a ocorrência de eventual ato ilícito praticado por meio da assinatura digital de documentos eletrônicos, quando o certificado digital já se encontra revogado. Considerando a dependência cada vez maior dos tribunais dos sistemas de informação, a garantia da autenticidade, integridade e confiabilidade dos documentos eletrônicos por meio dos quais os atos judiciais são praticados é relevante para a adoção do processo judicial eletrônico no tribunal estudado, contribuindo para a celeridade e efetividade na entrega da prestação jurisdicional e para a eficiência das atividades administrativas.

Studer (2007) (dissertação intitulada "**Processo judicial eletrônico e o devido processo legal**"), discutiu a legalidade e eficiência do Processo Eletrônico. Para tanto, levantou três hipóteses: (i) no que se refere à segurança das informações que trafegam na internet, entende-se que existem vários sistemas que podem garantir o tráfego destas, como a certificação digital, cadastro prévio dos usuários com utilização de senhas, assinaturas digitais e outros; (ii) quanto à legalidade da implantação do processo eletrônico, a legislação a respeito da matéria é suficiente para autorizar o uso do processo inteiramente digital; (iii) o procedimento utilizado no processo eletrônico bem como o uso da certificação digital e assinatura digital estão de acordo com o devido processo legal.Com base em uma análise de referencial teórico, confirmou suas hipóteses em que verifica que a tecnologia da informação está sendo implantada no Poder Judiciário, culminando com a implantação do processo virtual, o qual já é realidade em algumas unidades jurisdicionais, estando de acordo com os ditames dos princípios do devido processo legal.

Deliberador (2004) (dissertação intitulada "**Um componente computacional para auxiliar o desenvolvimento de uma assinatura digital no sistema de informações processuais**"), desenvolve um componente computacional em forma de pacote (*package*), utilizando a linguagem de programação Java, que auxiliará desenvolvedores de sistemas de computador a integrar a técnica da assinatura digital ao SIP. Conclui que o componente computacional proposto, possibilita implementar as técnicas de assinatura digital em diversos módulos do SIP, aperfeiçoando a segurança do sistema, possibilitando que seus usuários possam assinar digitalmente todo e qualquer trâmite processual e posteriormente realizar a verificação de validade da assinatura inserida.

Ishikawa (2003) (dissertação intitulada "**Um modelo computacional para o funcionamento da assinatura digital no sistema de informatização processual**"), propõe um modelo computacional que possibilite a integração da técnica da assinatura digital no Sistema de Informatização Processual (SIP), desenvolvido pelo Tribunal Regional do Trabalho 14ª Região Rondônia/Acre em parceria com o Departamento de Expressão Gráfica da Universidade Federal de Santa Catarina, a fim de aperfeiçoar a segurança do sistema atual e garantir a integridade e a autenticação informatizada de todo e qualquer trâmite processual criado ou alterado pelos usuários do sistema. Conclui que os usuários do (SIP) poderão contar com mais um recurso de segurança – as assinaturas digitais – que possibilitará a

autenticação informatizada de todos e quaisquer trâmites processuais, pois permite a realização de mais tarefas, o que lhe agrega valor, e terá sua confiabilidade incrementada, o que o coloca na classe dos sistemas adaptados às novas necessidades que a própria dinâmica dos tempos de Internet impõem.

Rockembach (2009) (dissertação intitulada "A implantação da assinatura digital no Tribunal Regional Federal da Quarta Região: perspectiva infocomunicacional"), buscou avaliar de que forma os desembargadores do tribunal utilizam a assinatura digital e verificar se esta implantação trouxe dinamicidade ao fluxo informacional, onde conclui que o impacto causado com substituição do suporte papel que contém uma assinatura manuscrita, para a assinatura digital, implica a preocupação com uma série de fatores, como disseminação, conscientização e capacitação, capazes de transpor as barreiras culturais que existem nestas mudanças.

**Saúde**

Kobayashi (2007) (tese intitulada "**Abordagem criptográfica para integridade e autenticidade em imagens médicas**"), propõe uma nova abordagem para imagens médicas, utilizando mecanismos de criptografia de imagem para conferir integridade e autenticidade "fortes". Afirma que a integridade e a autenticidade de imagens médicas são fatores bastantes críticos, na medida em que fornecem mecanismos para evitar e minimizar a adulteração de informações acerca do paciente, auxiliando a prevenir erros que podem causar prejuízos de ordem física e moral ao paciente. Assim, propôs um modelo a partir do padrão DICOM, estabelecido para a transmissão e armazenamento de imagens médicas. A implementação e testes comparativos de desempenho revelaram que o algoritmo possui uma boa relação custo-benefício, oferecendo um grau adicional de segurança à assinatura digital sem acarretar uma perda de performance significativa.

Eid (2007) (dissertação intitulada "**Avaliação do conhecimento e utilização da certificação digital em clinicas de radiologia odontológica**"), investiga o conhecimento e utilização da certificação digital em Clínicas de Radiologia Odontológica, que disponibilizam a seus clientes arquivos no formato eletrônico. Os resultados da pesquisa são frutos da elaboração de um questionário, aplicado a 450radiologistas de todo Brasil que tinham seus dados registrados junto ao Conselho Federal de Odontologia. O questionário continha perguntas sobre o nível

de informatização das clínicas radiológicas e o grau de conhecimento em certificação digital. De acordo com os resultados, todos os radiologistas entrevistados utilizavam, em suas clínicas radiológicas, arquivos no formato eletrônico, porém o uso da assinatura eletrônica em seus documentos digitais ainda é baixo. Dos 158 questionários respondidos, 79,1% dos entrevistados afirmaram que tinham dúvidas sobre como adquirir os certificados digitais e desconheciam o custo total para a sua aquisição. Conclui que os arquivos no formato eletrônico são utilizados nas Clínicas de Radiologia Odontológica, entretanto a Certificação Digital é pouco empregada para assiná-los. Pouco se conhece sobre a Certificação Digital, bem como a sua utilização, o que sugere necessidade de maior divulgação de sua importância pelas estruturas governamentais ou Conselhos da classe odontológica.

Nobre et al. (2007) (artigo intitulado "**Certificação digital de exames em telerradiologia: um alerta necessário**"), apresentam um estudo em telerradiologia que evidencia a importância do uso da certificação digital em documentos clínicos eletrônicos (laudos e exames). Justificam essa importância apresentando em números as fraudes eletrônicas ocorridas entre os anos 2004 e 2005, quando não havia a inclusão da certificação digital nos documentos clínicos eletrônicos, que aumentaram em 579%. Com a certificação digital tem-se, em relação aos sistemas de imagens digitais, por exemplo, que, em médio prazo, proporciona redução de custos, favorecendo uma menor utilização de filmes e químicos, e diminuindo a repetição de exames, seja por questões técnicas ou seja por permitir o acesso facilitado a exames anteriores de um determinado paciente. Além disso, proporciona o intercâmbio facilitado de exames e resultados, o que torna imediatamente disponível a opção da troca de serviços de laudo entre clínicas e a criação de centrais de telediagnóstico.Com o objetivo de esclarecer e informar aos médicos esses novos procedimentos, apresentam as ferramentas de segurança na área, que estão divididas em três grupos com características e ações distintas: acesso seguro, assinatura eletrônica e protocolação digital; formando o "tripé da segurança em telerradiologia" (TST).Concluem que para sua implementação é necessário tratar de questões de segurança, sobretudo em relação à privacidade, idoneidade, temporalidade das informações trafegadas, garantia de integridade de seu conteúdo, bem como do momento de sua geração, transmissão, manipulação e armazenamento. Aspectos esses em que a certificação digital tem exercido um papel positivamente.

Borges (2003) (dissertação intitulada "**Ferramenta de comunicação e acesso remoto a imagens médicas**"), desenvolve uma ferramenta computacional (*software*) que permite a captação, transmissão, leitura, edição e armazenamento remoto de dados biomédicos, com critérios de segurança, autenticação, autorização e integridade de dados. Seu principal objetivo é mostrar a possibilidade de edificação de *softwares* de acesso e controle remoto de dados biomédicos baseados em sistemas de segurança e permissão seletiva. A aplicação segue um modelo de requisição de serviços cliente-servidor, sob uma arquitetura em camadas, escrita na linguagem de programação Java com as seguintes funcionalidades: visualização de imagens médicas no formato DICOM (*Digital Imaging and Communications in Medicine*); edição remota de laudos com assinatura digital; armazenamento de dados relativos ao paciente (demográficos e imagens) e transmissão de imagens médicas. A autora acrescenta que o uso de chaves criptográficas "fortes" pode ser um incremental importante a ser desenvolvido, assim como à obediência completa a padrões de uma VPN (Rede Privada Virtual), visto o *software* ser passível de utilização através de uma rede pública, como a internet, para comunicação interinstitucional.

**Outras aplicações**

Moecke (2011), em sua dissertação intitulada "**NBPKI: uma ICP baseada em autoridades notariais**", propôs uma nova abordagem de Infraestrutura de Chaves Públicas adequada para conservação em longo prazo de assinaturas digitais, sem perder a generalidade esperada de uma ICP. Após analisar o modelo de negócio da ICP-Brasil, o autor apresenta soluções para os problemas identificados e argumenta que neste modelo a ICP-Brasil: a) tenha uma complexidade baixa de processamento exigido para validação de uma assinatura digital, em especial para o signatário e verificador; b) exija uma quantidade mínima de informações para ser validada com segurança; c) assinaturas digitais sejam de simples manutenção e conservação a longo prazo; d) mantenha-se a generalidade de uso de uma ICP; e) possua mecanismos de segurança adequados para a comprovação legal da autenticidade de assinaturas digitais. Em linhas gerais, conclui que o modelo proposto possibilita reduzir a dificuldade de validação de uma assinatura digital, em que o certificado do usuário deve ser autoassinado, e a Autoridade Certificadora seja substituída por uma Autoridade Notarial. Este modelo

elimina a cadeia de certificação do usuário e assume como parte do modelo a obtenção de provas de validade do certificado. E por fim, este modelo reduz a quantidade de código a ser implementado em um verificador de assinaturas digitais, e pode acelerar o desenvolvimento de aplicações baseadas em ICP, em especial para dispositivos com recursos limitados como sensores e telefones móveis.

Romani (2009) (dissertação intitulada "**Integração de serviços de relógio para Infraestrutura de Chaves Públicas**"), desenhou uma solução para a integração dos serviços de relógio no contexto de uma Infraestrutura de Chaves Públicas (ICP). Para tanto, estudou as principais entidades certificadoras e seus serviços, tais com a americana Verisign e a brasileira ICP-Brasil, e fez uma visita ao Observatório Nacional do Rio de Janeiro (ON), onde se conheceu as instalações do serviço de tempo. Ele conclui que para os serviços de carimbo de tempo, de hora e de criptografia temporal é essencial que a hora utilizada nesses serviços seja segura e confiável. Para se obter uma hora confiável é necessário que o relógio, que é utilizado ao se gerar a informação temporal, esteja sincronizado com uma fonte Confiável de Tempo – FCT. Para se ter um relógio seguro, o uso de um hardware criptográfico é necessário. A utilização de um hardware criptográfico na gestão do relógio protege o relógio do meio exterior e garante o correto funcionamento para ser utilizado pelos serviços de tempo, sendo ideal o uso de um único módulo que realiza a gestão do relógio, e provê os serviços de tempo que necessitam utilizar esse relógio seguro, como o serviço de carimbo de tempo, serviço de hora e serviço de criptografia temporal.

Fernandez (2010) (tese intitulada "**Proposta de um sistema eletrônico embarcado para fiscalização automática de veículos rodoviários de carga**"), coloca que as aplicações com certificado digital têm sido inseridas em diversas situações como em sistemas eletrônicos para fiscalização automática de veículos rodoviários de carga. Assim, para a identificação inequívoca do condutor é realizada por meio de uma estrutura de certificação digital baseada em cartões inteligentes, garantindo também a privacidade das informações.

2.3.4.3 Publicações com viés crítico à certificação digital no Brasil

Ferreira (2010) (dissertação intitulada "**O sistema de certificação digital brasileiro frente ao princípio da livre concorrência**"), objetivou desenvolver uma análise crítica fundamentada do modelo nacional de certificação digital implantado pelo Governo Federal, buscando enfrentar a questão nuclear do trabalho, que consiste em responder se o sistema nacional de certificação digital brasileiro viola o princípio constitucional da livre concorrência. Sob as diversas óticas pesquisadas demonstrou que a atipicidade crônica que embasou a ICP-Brasil é permeada de questionável legalidade, pois foi instituída a partir de atos inadequados, imperfeitos e incompletos. Conclui que o sistema de certificação digital implantado pelo Governo Federal resulta em interferência indevida na atividade econômica, viola o princípio da livre concorrência e retira a autonomia da iniciativa privada; e finaliza observando que a concorrência desleal implantada pelo Estado pode vir a sedimentar um monopólio estatal.

Bertol (2009) (tese intitulada "**Uma proposta para Regulamentação da Certificação Digital no Brasil**"), analisou os regulamentos da ICP-Brasil e apontou aqueles que devem ser criados ou alterados para que os documentos assinados digitalmente com chaves provadas associadas a certificados digitais ICP-Brasil reúnam condições técnicas necessárias e suficientes para serem úteis como evidência legal, mesmo no longo prazo. Para isso, realizou pesquisa bibliográfica, análise e comparação da legislação brasileira com a da comunidade Européia e calcou-se também, fortemente, na observação detalhada dos processos adotados na ICP-Brasil, durante os sete anos em que a autora trabalhou na AC-Raiz, inicialmente na Coordenação de Auditoria e Fiscalização e nos últimos três anos na Coordenação de Normalização e Pesquisa. Tratando-se de aspectos mais técnicos que envolvem a ICP-Brasil, propôs a inclusão de adequações nos regulamentos e na estrutura da ICP-Brasil.

Guelfi (2007) (dissertação intitulada "**Análise de elementos jurídico-tecnológicos que compõem a assinatura digital certificada digitalmente pela Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil)**"), abordou os elementos jurídico-tecnológicos que compõem a assinatura digital certificada pela ICP-Brasil. Para tanto, traçou dois grandes objetivos, um deles relacionado ao aspecto jurídico da certificação digital, levando em consideração a possibilidade do certificado digital conferir ou não presunção de legitimidade quanto a

autoria do documento eletrônico; e um segundo objetivo de caráter tecnológico, que se baseou no estudo de problemas encontrados na utilização dos algoritmos de função de *hash* pela ICP-Brasil. A fim de alcançar os objetivos propostos trouxe um arcabouço teórico denso sobre normativas e aspectos técnicos da certificação digital. A partir da análise do referencial teórico, conclui, sob o aspecto jurídico, que a medida provisória 2.200-2/01 é inconstitucional, uma vez que não respeita a regra de competência material fixada pela Constituição da República Federativa do Brasil para desenvolvimento da atividade notarial. Já sob o aspecto tecnológico, sabe-se que os algoritmos de função *hash* MD5 e SHA-1 tem seu papel na assinatura digital para garantir a integridade dos documentos eletrônicos; contudo, em 2004 o MD5 foi quebrado, possibilitando a realização de assinaturas digitais forjadas. Neste mesmo ano foram encontradas algumas fragilidades no SHA-1, mas que não inviabilizaram o seu uso para assinaturas digitais. Mesmo com essas evidências a ICP-Brasil adotou até 2006 o algoritmo de função *hash*MD5. Além disso, as assinaturas digitais realizadas com o MD5 até maio de 2006 podem ser perfeitamente forjadas sem deixar vestígios e ainda assim possui valor jurídico.

Demócrito (2005) (artigo intitulado "**A ICP-Brasil e os poderes regulatórios do ITI e do Comitê Gestor**"), visou comprovar, através da análise das atribuições conferidas ao ITI e ao Comitê Gestor da ICP-Brasil, que esses órgãos, em conjunto, atuam com características próprias de agências reguladoras, no que diz respeito às atividades de certificação digital no Brasil. Conclui que o "marco regulatório" da atividade de certificação digital no país coincide com a edição da MP 2.200, o primeiro texto legal a disciplinar a estrutura da ICP-Brasil, em que o conjunto de atribuições que foram conferidos ao Comitê Gestor e ao ITI demonstra que esses dois órgãos, em conjunto, desempenham tarefas que, a despeito das peculiaridades, se incluem como atividades típicas de uma agência reguladora, por possuírem poder gerencial (técnico) e de controle sobre os prestadores de serviços de certificação credenciados. Sua atuação (em conjunto ou isoladamente) revela intervenção estatal junto a um setor privado, para impor normas de conduta a particulares que visem o bem-estar coletivo. O Comitê Gestor e o ITI não têm atribuição de regular a atividade de certificação digital como um todo, mas qualquer prestador de serviços que tiver interesse em expedir certificados com validade jurídica contra terceiros, terá que se credenciar junto a ela e, consequentemente, se submeter a seus poderes regulatórios.

Silvestre (2003) (dissertação intitulada "**A ilegitimidade constitucional crítica da infraestrutura de chaves públicas brasileiras: uma semiótica do poder**"), objetivou demonstrar que a utilização de ferramental e conceitos tecnológicos atuais deve guardar direta relação com os mecanismos jurídicos de legitimação implementar, bem como respeitar os paradigmas de transição semióticos ocorrentes a medida em que se intercambiam as demandas físicas com soluções virtuais. Observando a ocorrência desta fenomenologia na constituição da ICP-Brasil, analisa o cenário socioeconômico. Ao analisar as normas da ICP, apresenta duas contradições constitucionais relevantes: a) a análise da documentação legal determinou que o Poder Executivo utilizasse deliberadamente de uma Medida Provisória para, exclusivamente inovar o cenário legal/constitucional, exercendo o poder legislativo ordinário, ainda que potencialmente urgente; b) ainda que a urgência e relevância do caso determinasse pela produção legislativa, o corpo jurídico provisório é insuficiente para garantir a operacionalidade segura da ICP-Brasil, sendo, portanto, supérflua e ineficiente, uma pré-existência jurídica, antes da conscientização cultural dos usuários e de uma infraestrutura com moldes democraticamente elaborados. Define o seguinte conjunto de valores como núcleo principal da estrutura pública instituída: a) Modelização de uma infraestrutura de chaves públicas única, com uma única Autoridade Certificadora Raiz com sistema de certificação digital operando assinaturas eletrônicas usando algoritmos de criptografia assimétrica (chave pública e privada), com sustentação legal, estabilizado pelo tempo constitucional, destinado a operar um mercado de prestação de serviços e comercialização de chancelas eletrônicas, atendendo também e concomitantemente todos os níveis do Estado; b) Ausência de Agência e Norma Reguladora capaz de mediar uma ética regulamentar e as disputas entre a predominância da ICP-Brasil e outros potenciais atores; c) Implantação de um modelo de mercado aberto e de livre concorrência, com dois níveis de qualidade de produto, segundo uma vinculação credencial a ICP-Brasil, criando um desnível legal de credibilidade, inclusive internacional, tanto pela predominância institucional deste ator, como pela construção de uma primeira ação de marketing dominante; d) Implantação de presunção jurídica de qualidade e segurança nos serviços da ICP-Brasil; e) Instauração do princípio da exclusividade, determinando uma pré-imputação do ônus da prova aos usuários, limitando-se a responsabilidade civil dos prestadores de serviço, bem como sua obrigação informacional, coisa conflitante com o Código de Defesa do Consumidor; f) Implanta, por analogia presuntiva, força de validade aos

documentos eletrônicos, assimiláveis ao preceito do artigo 131 do Código Civil. Faz a análise de 48 textos sobre a temática e divide em 11 áreas temáticas, considerando o nº de ocorrências, onde verifica-se que o maior tema de discussão é a validade jurídica dos documentos digitais e o menor é Programas de Educação para Técnicos Usuários na ICP. Conclui dentre outras questões que a tecnologia e seus desdobramentos na vida do indivíduo estabelecem novos parâmetros culturais de consumo, dos produtos e dos comportamentos, sendo a intermediação deste relacionamento um negócio rentável e mercadologicamente reservado; onde a implantação de um Governo Eletrônico não corresponde ao e-commerce em larga escala, nem a implantação do Governo físico, este já existe e sempre existirá. O conceito eletrônico introduzirá o cidadão na governabilidade, fiscalizando, propondo, votando, enfim denunciando o trato da coisa pública. Afirma ainda que, com a criação de mais um espaço reservado, instituído por nova legalidade de ocasião, ganha fôlego econômico e político o Executivo, pois que podendo licitar a terceiros a execução dos trabalhos, renova o compartilhamento privatizante de atividades essencialmente públicas e estratégicas, como é o ciberespaço.

#### 2.3.4.4 Publicações sobre o impacto da certificação digital no Brasil

Os artigos encontrados na busca sistemática desta pesquisa, que trataram do impacto da certificação digital, versaram basicamente sobre questões de governo eletrônico e políticas públicas, onde foram identificadas como potencialidades que a certificação traz: (1) promove a segurança aos dados de programas governamentais, da tramitação de processos e demais transações eletrônicas; (2) facilita a arrecadação de impostos; (3) assegura um melhor controle dos programas de governo; (4) dá mais celeridade à tramitação de processos; (5) aumenta a transparência das ações governamentais; (6) promove a desmaterialização dos processos; (7) economia de tempo; (8) bem como autenticidade, confidencialidade e integridade de dados, validade jurídica, entre outras questões.

De forma sucinta, as publicações que trataram do impacto da certificação digital no Brasil (5 publicações analisadas, sendo 3 artigos e 2 dissertações), são:

Alonso, Ferneda e Braga (2011) (artigo intitulado "**Governo eletrônico e políticas públicas: análise sobre o uso da certificação digital no Brasil**"), investigam a relação entre governo eletrônico, especificamente o uso da certificação digital, e a melhoria do processo de formulação e implantação de políticas públicas brasileiras. Os resultados obtidos com relação ao potencial de aperfeiçoamento do processo de formulação e implantação de políticas públicas com uso de certificação digital, foram: prover segurança aos dados de programas governamentais, facilitar a arrecadação de impostos, proporcionar segurança na tramitação de processos, assegurar um melhor controle dos programas de governo, garantir segurança nas transações eletrônicas, dar mais celeridade à tramitação de processos, aumentar a transparência das ações governamentais. Colocam que, haja vista estes potenciais da certificação digital em prol do aperfeiçoamento da implantação de políticas públicas, ainda não ocorre o mesmo com o processo de formulação de políticas com participação popular como, por exemplo, uma votação direta com a segurança de uma assinatura digital, a fim de influenciar na criação de uma determinada política. Ou seja, trata-se ainda de uma possibilidade de melhoria em potencial do processo. Sua concretização futura poderá representar a participação efetiva da sociedade nos processos políticos, fortalecendo a democracia e ampliando a cidadania. Esta lacuna pode estar relacionada a dois fatores: o estágio mediano de desenvolvimento do governo eletrônico brasileiro e o elevado grau de exclusão digital verificado no País. A existência dessas possíveis correlações enseja a realização de trabalhos futuros com o objetivo de estabelecer em que medida o processo de formulação de políticas pode ser alterado pelo avanço da inclusão digital e pelo nível de desenvolvimento do governo eletrônico no Brasil.

Braga (2011) (artigo intitulado "**O impacto do governo eletrônico sobre a prestação de serviços públicos no Brasil: aplicações da certificação digital**"), analisa o impacto do governo eletrônico, particularmente as aplicações da tecnologia de certificação digital, sobre a prestação de serviços públicos no Brasil, através de entrevistas com dez atores-chave brasileiros, seguida de uma análise de conteúdo sobre possibilidades do emprego da certificação digital como suporte ao desenvolvimento do governo eletrônico brasileiro, especificamente enquanto ferramenta que viabiliza a ampliação e melhoria dos serviços públicos. Os resultados mostram que as principais vantagens do uso da certificação digital se relacionam a questões concernentes à segurança da informação, assim como aos aspectos que dizem respeito a seus requerimentos, quais sejam, autenticidade,

confidencialidade e integridade de dados, ou seja, a certificação digital guarda uma relação direta com a segurança da informação. A qualidade de aperfeiçoar e ampliar o acesso aos serviços públicos, sem necessidade da presença física, tornando os procedimentos mais céleres e transparentes e economizando recursos, são descritos atributos do governo eletrônico.

Fukushima (2010) (dissertação intitulada "**Aplicabilidade de Certificados de Atributo no Âmbito da ICP-Brasil**", analisa a aplicabilidade da tecnologia de certificados de atributo, em operação conjunta com os certificados digitais de identidade emitidos no âmbito da ICP-Brasil, apresentando os principais desafios na implementação desta tecnologia, assim como o perfil de uso do certificado de atributo (CA) mais adequado às necessidades das aplicações relacionadas ao processo de autenticação e atribuição de privilégios. Apresenta diversos estudos de caso e conclui que, pela necessidade de prover segurança aos sistemas, relacionada à identificação e à qualificação do usuário, muitas entidades têm adotado a tecnologia de certificados de identidade com atributos nas suas infraestruturas, porque não existe um conhecimento disseminado da tecnologia dos certificados de atributo. Este trabalho reforça as vantagens da separação de uma infraestrutura específica para o mecanismo de autenticação (ICP)e outra específica para a qualificação (IGP). Em relação à viabilidade da adoção de certificados digitais destaca os seguintes quesitos: segurança, gestão dos atributos e certificados, legalidade, e interoperabilidade.

Braga (2008) (artigo intitulado "**O impacto do governo eletrônico sobre a prestação de serviços públicos no Brasil: aplicações da certificação digital**"), analisa relação entre o desenvolvimento de práticas de governo eletrônico, especificamente a certificação digital, e o possível aperfeiçoamento da prestação de serviços públicos no país. Conclui que a certificação digital guarda uma relação direta com a segurança da informação, que por sua vez, é condição necessária ao desenvolvimento do governo eletrônico, e ainda, mantém uma relação indireta com a melhoria dos processos da Administração Pública e da qualidade de interface do Estado com o cidadão, aspectos estreitamente vinculados à melhoria dos serviços públicos. Coloca que a qualidade de aperfeiçoar e ampliar o acesso aos serviços públicos, sem necessidade da presença física, tornando os procedimentos mais céleres e transparentes e economizando recursos são descritos como atributos do governo eletrônico e não da certificação digital.

Ainda Braga (2008) em sua dissertação intitulada "**Contribuições da certificação digital ao desenvolvimento do governo eletrônico e aperfeiçoamento de políticas públicas e serviços públicos no Brasil**", examinou o papel desempenhado pela certificação digital na evolução do processo de formulação e implantação de políticas públicas e serviços públicos, por intermédio de ações do Governo Eletrônico Brasileiro. Apresenta como **vantagens** da certificação digital: assegura a segurança das informações eletrônicas; proporciona autenticidade aos dados eletrônicos; confere validade jurídica aos documentos eletrônicos; garante a confidencialidade dos dados e das transações eletrônicas; provê integridade aos dados eletrônicos; desburocratiza os procedimentos administrativos; melhora a eficiência (celeridade); desmaterializa os processos físicos; auxilia o controle e a auditoria; prescinde da presença física nas interações com o governo; economia de tempo; e facilita o acesso aos serviços públicos. Percebe que não foi indicada nenhuma possível desvantagem de seu uso (cultural, infraestrutura e logística, existência de poucas aplicações, custo elevado, dificuldade de acesso, difícil compreensão da tecnologia envolvida). Apresenta como principais **possíveis usos** da certificação digital pelo governo eletrônico: Promoção de uma melhor interação do Estado com o cidadão; Autenticação segura para acesso a serviços públicos; Autenticação de bases de dados; e Tramitação eletrônica de documentos. Como **potencial de aperfeiçoamento de políticas públicas** através do uso da certificação digital coloca que a certificação digital permite: Prover segurança às bases de dados de programas governamentais; Facilitar a arrecadação de impostos, proporcionar segurança na tramitação de processos; Assegurar um melhor controle dos programas de governo; Garantir segurança nas transações eletrônicas; Dar mais celeridade à tramitação de processos; e Aumentar a transparência das ações governamentais. Percebe como **perspectivas futuras**: Prestação de mais serviços públicos eletrônicos; Disponibilização de identidade digital; Substituição do processo físico pelo eletrônico; Aumento da eficiência estatal; Transição do sistema presencial para o virtual; Incremento das transações em meio eletrônico; Arquivamento de dados de forma mais sustentável; Transformação da cultura burocrática; Massificação do uso da certificação digital. Coloca que os serviços públicos podem disseminar o uso da certificação digital através: do aumento do rol de serviços públicos eletrônicos; da realização de campanhas informativas na mídia; lançando mão de parcerias interinstitucionais; fomentando novas aplicações; melhorando a logística; capacitando pessoal em certificação digital. Conclui que a

certificação digital guarda relação direta com a segurança da informação, que é condição necessária ao desenvolvimento do governo eletrônico e uma relação indireta com a melhoria dos processos da Administração Pública e da qualidade de interface do Estado com o cidadão, aspectos estreitamente vinculados à melhoria dos serviços públicos e aperfeiçoamento do processo de formulação e implantação de políticas públicas. Conclui ainda, que, embora a certificação digital seja apontada como responsável por maior economia, celeridade, comodidade, entre outros, na realidade estes são benefícios advindos do uso das TIC's.

A partir da análise dos artigos que trataram sobre o impacto da certificação digital no Brasil pode-se identificar que os impactos identificados na área de governo eletrônico, são basicamente intrínsecos à tecnologia.

Em relação às aplicações com uso da certificação digital no Brasil, observa-se que são basicamente desenvolvidas também entorno de governo eletrônico, como veremos na próxima subseção.

### 2.3.5 Aplicações da certificação digital no Brasil

No Quadro 2, apresentam-se algumas das principais aplicações com uso de certificação digital ICP-Brasil.

Observa-se que estas são iniciativas do governo e que pelo menos a cada 1 ou 2 anos o governo lança uma nova aplicação com utilização obrigatória da certificação digital.

**Quadro 2: Algumas aplicações com certificação digital**

| Ano | Aplicação | Instituição | Objetivos | Benefícios |
|---|---|---|---|---|
| 2002 | Sistema de Pagamentos Brasileiro (SPB) | BC - Banco Central do Brasil | Gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, interligando as instituições financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas. Tem o objetivo de permitir a transferência de recursos, o processamento e a liquidação de pagamentos para pessoas físicas, empresas e governos, ou seja, aumentar a segurança do mercado, oferecendo maior proteção contra possíveis rombos ou quebra em cadeia (efeito dominó) de instituições financeiras. | Possibilidade de transferência imediata de dinheiro; Agilidade (os recursos ficam disponíveis no dia da transferência). Segurança e confiabilidade (redução do risco de crédito nos pagamentos, que são irreversíveis (não podem ser sustados ou devolvidos por falta de fundos, como pode ocorrer com cheques)) |
| 2002 | Sistema do Banco Central do Brasil (SISBACEN) | BC - Banco Central do Brasil | Sistema de Informações Banco Central é um sistema eletrônico de coleta, armazenagem e troca | Permite conexão direta à rede de computadores do Banco Central do Brasil; conexão |

| | | | | |
|---|---|---|---|---|
| | | | de informações que liga o Banco Central aos agentes do sistema financeiro nacional. Visto ser obrigatório o registro de todas as operações de câmbio realizadas no País, o Sisbacen é o principal elemento de que dispõe o Banco Central para monitorar e fiscalizar o mercado. | via rede privada de provimento de serviços de acesso ao Sisbacen; conexão via internet (apenas para usuários governamentais, usuários especiais, Cooperativas de Crédito, Sociedades de Crédito ao Microempreendedor e Administradoras de Consórcios) |
| 2004 | Programa Universidade para Todos (PROUNI) | MEC - Ministério da Educação | Iniciativa do Ministério da Educação (MEC) que concede bolsas de estudo integrais e parciais a estudantes de baixa renda. O sistema é acessado pela instituição de ensino superior por meio de certificado digital. | Além de garantir total segurança às informações cadastradas no Sisprouni, o uso da certificação digital possibilita o registro de assinatura digital em todos os documentos emitidos, o que dispensa o envio desses por via postal, bem como o reconhecimento de firma dos signatários. |
| 2005 | Central Virtual de Atendimento ao Contribuinte (e-CAC) | RFB - Receita Federal do Brasil | O Portal e-CAC é um portal eletrônico onde diversos serviços protegidos por sigilo fiscal podem ser realizados via internet pelo próprio | Oferece consulta da situação fiscal dos contribuintes, prestação de contas, procuração eletrônica, entre outros; |

| | | | | |
|---|---|---|---|---|
| | | | contribuinte, tais como: verificar eventuais pendências na Declaração do Imposto de Renda Pessoa Física, obter cópia de declarações, retificar pagamentos, parcelar débitos, pesquisar a situação fiscal e imprimir o comprovante de inscrição no CPF. Sua utilização requer Código de Acesso ou Certificado Digital, porém, alguns serviços estão disponíveis apenas para usuários que estiverem fazendo uso de Certificado Digital. | |
| 2006 | Restrições Judiciais de Veículos Automotores (RENAJUD) | CNJ - Conselho Nacional de Justiça e Departamento Nacional de Trânsito - DETRAN | É uma ferramenta eletrônica que interliga o Judiciário e o– DENATRAN, possibilitando a efetivação de ordens judiciais de restrição de veículos cadastrados no Registro Nacional de Veículos Automotores – RENAVAM, em tempo real. | O tratamento eletrônico de ordens judiciais pelo sistema possibilita a visualização das respostas na tela e oferece recursos úteis para a tomada de decisão da autoridade judiciária.<br>Celeridade e economia processuais;<br>Garante o pagamento das dívidas judiciais com maior rapidez e segurança |

| | | | | |
|---|---|---|---|---|
| 2006 | Portal de Compras do Governo Federal (COMPRASNET) | MPOG - Ministério do Planejamento, Orçamento e Gestão | Nesse sistema de compras do Governo Federal, administrado pelo Ministério do Planejamento, Orçamento e Gestão, todos os pregoeiros utilizam a certificação para encaminhar os processos de compras governamentais feitos na modalidade pregão eletrônico. | Traz vantagens como:<br>Transparência;<br>Redução dos preços pagos pelo Governo;<br>Diminuição da diferença entre preços pagos pelos órgãos por produtos semelhantes;<br>Agilização e simplificação do processo de aquisição de bens e serviços comuns;<br>Redução dos custos operacionais do Governo e dos fornecedores;<br>Disponibilização rápida de informações gerenciais para dirigentes dos órgãos bem como para o alto escalão do Governo do Estado;<br>Maior interação entre fornecedores e Administração Pública Estadual;<br>Ampliação das oportunidades de negócios dentro do Estado;<br>Incremento da competição entre fornecedores;<br>Oportunidades para pequenos fornecedores; |

| | | | | |
|---|---|---|---|---|
| | | | | Proporciona à sociedade condições efetivas para o acompanhamento e fiscalização das compras governamentais. |
| 2006 (algumas empresas) 2010 (todas as empresa acima de 10 funcionários) | Nota Fiscal Eletrônica (NF-e) | RFB - Receita Federal do Brasil | Facilitar a vida do contribuinte e as atividades de fiscalização sobre operações e prestações tributadas pelo Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e pelo Imposto sobre Produtos Industrializados (IPI). Os estabelecimentos estão implantando o documento fiscal eletrônico e, assim, substituindo a emissão do documento fiscal em papel. | A empresa emissora de NF-e gerará um arquivo eletrônico contendo as informações fiscais da operação comercial, o qual deverá ser assinado digitalmente, de maneira a garantir a integridade dos dados e a autoria do emissor. Este arquivo eletrônico, que corresponderá à Nota Fiscal Eletrônica (NF-e), será então transmitido pela Internet para a Secretaria da Fazenda de jurisdição do contribuinte que fará uma pré-validação do arquivo e devolverá um protocolo de recebimento (Autorização de Uso), sem o qual não poderá haver o trânsito da mercadoria. A NF-e também será transmitida para a Receita Federal, que |

| | | | | |
|---|---|---|---|---|
| | | | | será repositório nacional de todas as NF-e emitidas. |
| 2006 (Tribunais Regionais Federais) 2007 (CNJ) | Sistema de Informações ao Judiciário (INFOJUD) | Conselho Nacional de Justiça - CNJ e RFB Receita Federal do Brasil | É um serviço oferecido unicamente aos magistrados (e servidores por eles autorizados), que tem como objetivo atender às solicitações feitas pelo Poder Judiciário à Receita Federal.<br>A ferramenta está disponível apenas aos representantes do Poder Judiciário previamente cadastrados, em base específica da Receita Federal, e que possuam certificado digital emitido por Autoridade Certificadora integrante da ICP-Brasil. | Identificação do advogado perante os órgãos jurídicos, como inscritos na Ordem;<br>Possibilita a prática em meio eletrônico, como protocolar petições e laudos periciais;<br>Concessão e restrição de acesso: garantia de impedimento que pessoas não autorizadas possam acessar transações e serviços;<br>Atuação nos tribunais, fóruns e varas que já têm processo eletrônico, sem a necessidade de sair do escritório;<br>Redução de custos operacionais;<br>Ganho de dinamismo, comodidade e agilidade no dia-a-dia;<br>Horário de peticionamento não condicionado ao horário do Fórum – 24hs |
| 2007 | Registro Eletrônico de | CFM - Conselho Federal de | É uma poderosa ferramenta para os médicos proverem com | Permite o armazenamento e o compartilhamento seguro das |

| | | | | |
|---|---|---|---|---|
| | Saúde (RES) | Medicina | qualidade e segurança um cuidado integrado aos seus pacientes. Num contexto genérico, trata-se de um repositório eletrônico de informações em torno da saúde das pessoas, possibilitando um panorama de seus históricos clínicos. | informações de um paciente.<br>Reduz a possibilidade de erros médicos;<br>Proporciona ao médico a gestão de conhecimento dentro do seu próprio consultório, ampliando, inclusive, a eficácia das suas atividades gerenciais e burocráticas; e<br>Contribui para diminuição dos custos do setor, principalmente por meio da redução da superutilização (duplicação de exames de laboratório) e da má utilização de serviços (fraudes, erros diagnósticos). |
| 2007<br>2012 | Sistema Público de Escrituração Digital (SPED) | RFB - Receita Federal do Brasil | A escrituração fiscal das empresas de todos os portes devem ser enviadas para o fisco por meio de arquivos eletrônicos validados com a certificação digital. Já o SPED Contábil disponibiliza um programa no qual o Livro Diário é importado, assinado | Redução de custos com a dispensa de emissão e armazenamento de documentos em papel; redução de custos com a racionalização e simplificação das obrigações acessórias; uniformização das informações que o |

| | | | | |
|---|---|---|---|---|
| | | | digitalmente pelo representante legal e pelo contador; | contribuinte presta às diversas unidades federadas; fortalecimento do controle e da fiscalização por meio de intercâmbio de informações entre as administrações tributárias; redução de custos administrativos; aperfeiçoamento do combate à sonegação; possibilidade de troca de informações entre os próprios contribuintes a partir de um leiaute padrão |
| 2010 | Programa Processo Eletrônico[3] | Supremo Tribunal Federal - STF | É um programa institucional do Supremo Tribunal Federal que define estratégias e ações coordenadas para a consolidação do processo judicial eletrônico na Corte. O programa estabelece uma agenda de trabalho que inclui desenvolvimento de tecnologia, edição de atos normativos e parcerias institucionais. Seu | Conforto do advogado que poderá peticionar de onde estiver, sem a necessidade de se deslocar até o STF; economia com hospedagem e transporte; horário diferenciado para o protocolo de petições até as 24 horas (hora oficial de Brasília) do dia em que vence o prazo; celeridade processual; |

[3]<http://www.stf.jus.br/portal/cms/verTexto.asp?servico=processoPeticaoEletronica&pagina=Informacoes_gerais_apos_desligamento_v1>.

| | | | | |
|---|---|---|---|---|
| | | | objetivo é aproximar, integrar e inserir todos os agentes envolvidos (partes, advogados, Tribunais, PGR, AGU, defensorias e procuradorias, dentre outros), para uma gestão judiciária automática, simples, acessível, inteligente e, sobretudo, mais célere e mais econômica.<br>O escopo do programa vai além da digitalização dos processos. Em linguagem didática, a proposta é tornar eletrônicas todas as fases ou momentos do processo: (a) o peticionamento, (b) a tramitação, (c) as comunicações e (d) a finalização. Será necessário, para tanto, adotar, com o envolvimento de todos, novo fluxo de tarefas. | significativa redução do fluxo de pessoas nas unidades do Tribunal, o que diminui as filas de espera para os que vêm à Corte; diminuição do risco de incidentes no deslocamento físico dos documentos (furto de malotes, exemplificativamente); segurança jurídica proporcionada pela assinatura digital (autenticidade e integridade do documento); economia de tempo – os atos processuais das partes consideram-se realizados no dia e na hora de seu recebimento no e-STF. |
| 2011 | Sistema Integrado de Informações Previdenciárias (SIPREV) | MPAS - Ministério da Previdência e Assistência Social | É um sistema informatizado para ajudar estados e municípios na gestão e operação de seus Regimes Próprios de Previdência Social | O Siprev é um banco de dados onde cada estado e município insere informações cadastrais de seus servidores, além de possibilitar aos |

| | | | | |
|---|---|---|---|---|
| | | | já concebido para eliminar o uso de papel. É por meio dele que os institutos estaduais e as prefeituras prestam contas ao Ministério da Previdência dos benefícios pagos aos servidores aposentados. | gestores a disponibilização de extrato previdenciário aos servidores, concessão automatizada de benefícios e acesso ao Sistema de Óbitos da Previdência Social. |
| 2011 | Sistema de Diárias e Passagens (SCDP) | MPOG - Ministério do Planejamento, Orçamento e Gestão | É um sistema informatizado, acessado via internet, que integra as atividades de concessão, registro, acompanhamento, gestão e controle das diárias e passagens, decorrentes de viagens nacionais ou internacionais realizadas no interesse da administração. O Sistema está vinculado à observância da legislação correspondente e integrado com outros sistemas do Governo Federal – SIAPE, SIAFI e SIORG. | Promove a tramitação eletrônica dos documentos e utiliza a certificação digital para aprovação de viagens e pagamento de diárias. A certificação é usada para dar transparência ao processo e permitir a identificação inequívoca da autoridade que autorizou a despesa. |
| 2011 | Conectividade Social[4] | Caixa Econômica Federal - CEF | É um canal eletrônico de relacionamento. É moderno, | Simplifica o processo de recolhimento do FGTS; reduz |

[4]<http://www.caixa.gov.br/fgts/conectividade_social_ICP.asp>.

| | | | | |
|---|---|---|---|---|
| | | | ágil e seguro, facilmente adaptável ao ambiente de trabalho das empresas ou escritórios de contabilidade que desejam cumprir suas obrigações em relação ao FGTS. Cada usuário tem uma cesta de serviços adequada ao seu perfil, que lhe permite realizar transações eletrônicas no canal. Atualmente, é possível fazer pelo canal diversas transações, como a transmissão do arquivo do Sistema Empresa de Recolhimento do FGTS e Informações à Previdência Social (SEFIP) e da GRRF, visualizar e imprimir extratos, retificar incorreções cadastrais e comunicar o afastamento de empregados, dentre outras. | custos operacionais; disponibiliza um canal direto de comunicação com a CEF – agente operador do FGTS; aumenta a comodidade, segurança e sigilo das transações com o FGTS; reduz a ocorrência de inconsistências e a necessidade de regularizações futuras; aumenta a proteção da empresa contra irregularidades e facilita o cumprimento das obrigações da empresa relativas ao FGTS |
| 2012 | Homologações das Rescisões Trabalhistas (Homolognet) | MTE - Ministério do Trabalho e Emprego | É um sistema de homologação das rescisões contratuais on-line. Os cálculos automáticos facilitam a emissão do termo de rescisão pela empresa e | Possibilita ao MTE oferecer novos serviços relativos à elaboração e rescisão contratuais, disponibilizando funcionalidades que só podem |

| | | | | |
|---|---|---|---|---|
| | | | garantem tranquilidade ao trabalhador, pois os valores das indenizações serão validados por um sistema atestado pelo Ministério do Trabalho e Emprego (MTE). | ser oferecidas a partir da segurança da certificação digital |
| 2013 | Diário Oficial Eletrônico | SP - Governo do Estado de São Paulo | Dá cumprimento ao disposto no art. 37 da Constituição, dar publicidade aos atos oficiais, sejam os do Estado (por seus três poderes) ou os que tenham imposição legal de publicação, de empresas e outras instituições privadas (acesso universal). É o instrumento que dá validade aos atos nele publicados. perenidade, que significa E informa aos interessados acerca de atos oficiais já do conhecimento público (perenidade). Esse objetivo serve a ações administrativas e judiciais posteriores e à pesquisa, em particular a pesquisa histórica. | Os projetos em Certificação Digital da Imprensa Oficial são desenvolvidos para garantir segurança e autenticidade nos mais diversos tipos de transações eletrônicas. Simplificando a vida de instituições que precisam de agilidade nos seus processos, total sigilo das informações eletrônicas e consultoria especializada em Certificação Digital. |

Fonte: o autor

Observa-se que as aplicações estão fundamentalmente associadas a serviços públicos, evidenciando o papel do governo como fomentador da difusão e adoção da certificação digital e estão concentradas nos anos de 2006 e 2011.

Observa-se ainda, que a adesão à utilização da certificação digital ICP-Brasil surge de uma necessidade operacional de cada setor, ou como uma obrigatoriedade para atender às aplicações criadas pelo governo (IGTI, 2013).

Algumas aplicações, como o Sistema Público de Escrituração Digital (SPED), por exemplo, possuem projetos inter-relacionados, que geram novas aplicações.

### 2.3.5 Certificação Digital e assinatura eletrônica em outros países

A maneira adotada para a emissão de certificados digitais se deu de formas diferentes em muitos países ao longo dos anos, seja em relação ao tipo de infraestrutura adotada ou ao tipo de credenciamento das Autoridades Certificadoras, no caso do Brasil, a ICP-Brasil teve origem a partir do modelo alemão.

Por volta de 1997, os primeiros países começaram a regulamentar a certificação digital, como se pode observar na Quadro 3:

**Quadro 3: Regulamentação da certificação digital em alguns países**

| PAÍS | ANO | REGULAMENTAÇÃO | TIPO DE CREDENCIAMENTO DAS AC's |
|---|---|---|---|
| Itália | 1997 | Lei nº59 | Voluntário |
| Alemanha | 1997 | Signaturgesetz | Por Autoridade Credenciadora |
| EUA | 1998 | Regulamentações Estaduais e *Digital Signatureand Eletronic AuthenticationAct* | Não prevê |
| Espanha | 1999 | Diretiva 1999-93 | Voluntário |
| Portugal | 1999 | Decreto-Lei nº 290-D | Por Autoridade Credenciadora |

| | | | |
|---|---|---|---|
| Brasil | 2001 | MP 2.200-2 | Por Autoridade Credenciadora |

Fonte: conforme LINS (2005)

A assinatura digital começou a ser regulamentada basicamente junto com a certificação digital, sendo os EUA o único país a apresentar leis específicas para cada Estado.

A Quadro 4 apresenta as principais legislações de cada país.

**Quadro 4: Regulamentação da assinatura eletrônica em alguns países**

| PAÍS | ANO | LEI | LINK |
|---|---|---|---|
| Alemanha | 2001 | Signaturgesetz | http://www.certisign.com.br/documents/10163/690007a3-95f5-4bf8-a632-076bcb0e3e1a |
| Argentina | 2001 | Ley 25.506 | http://www.certisign.com.br/documents/10163/82372b9f-b7f9-4eb4-be7f-3b8cf98d7896 |
| China | 2004 | *Electronic Signature Law of the People's Republic of China* | http://www.certisign.com.br/documents/10163/fe6628f3-0d77-4fac-b0f2-7d07eb52ed64 |
| Colômbia | 1999 | Ley 527 | http://www.certisign.com.br/documents/10163/04b59a69-fccc-4a4f-ad6a-4ce65e199744 |
| Espanha | 2003 | Ley 59 | http://www.certisign.com.br/documents/10163/a2921636-8387-4e9f-97b1-1c8e1c15effd |
| EUA | 2001 | * | http://www.certisign.com.br/documents/10163/ee791b13-786b-4aee-b921-e28cc6350f01 |
| França | 2000 | LOI 2000-230 | http://www.certisign.com.br/documents/10163/58489291-0c67-46d8-b8f2-13f4a946761a |
| Itália | 2005 | *Codice dell'amministrazione digitale* | http://www.certisign.com.br/documents/10163/a7694b80-0bff-459c-9429-b65b2f761937 |
| Peru | 2000 | Ley 27.269 | http://www.certisign.com.br/documents/10163/ad25c594-b463-4c4c-acb9-7ba80cc99068 |
| Portugal | 1999 | Decreto-Lei 290-D/99 | http://www.certisign.com.br/documents/10163/87ab189c-5f3e-488c-b27b-d28cc403ccf5 |

| | | | |
|---|---|---|---|
| Reino Unido | 2000 | *Electronic Communications Act* | http://www.certisign.com.br/documents/10163/a3279f77-660f-44d5-b78f-0597fbd8baa7 |
| Venezuela | 2001 | Decreto com fuerza de Ley | http://www.certisign.com.br/documents/10163/06ec771b-f86f-4249-9741-6762d2fd59cf |

* Nos EUA cada Estado tem legislação própria.
Fonte: http://www.certisign.com.br/certisign/legislacao/internacional

Segundo a Celepar (2007) os principais modelos de ICP são:

> **Modelo Isolado**: Hierárquico com AC-Raiz única.
> **Modelo Floresta**: Várias ICP's independentes (pode ter certificação cruzada entre algumas AC-Raízes).
> **Modelo em Malha**: Semelhante a floresta, mas com certificação cruzada entre todas as AC-Raízes.
> **Modelo com Ponte**: Semelhante a floresta onde cada AC-Raíz tem certificação cruzada com uma entidade central denominada PONTE.
> **Modelo Internet**: AC-Raízes de certificados confiáveis pelo navegador já vem pré-instaladas.

No Brasil o modelo adotado foi o modelo Alemão, composto por uma Raiz Única, que de acordo com Celepar (2007) se configura como "modelo isolado".

Diversos países se preocuparam com a regulamentação da certificação digital no mesmo período e levaram relativamente o mesmo tempo para criarem a regulamentação também das assinaturas digitais.

Na próxima seção serão apresentados alguns modelos de adoção de inovações tecnológicas, a fim de servir de base para o entendimento de como se dá o processo de adoção de novas tecnologias.

## 2.4 MODELOS DE ADOÇÃO DE INOVAÇÕES TECNOLÓGICAS

Esta subseção tem por objetivo apresentar alguns modelos de adoção de inovações tecnológicas, uma vez que a maneira de adotar uma tecnologia impacta no sucesso ou fracasso desta tecnologia.

A adoção de tecnologias, tanto TI como TIC´s, têm influenciado substancialmente o processo de tomada de decisão, uma vez que a divulgação das comunicações está levando a uma espera menor de informação e resposta. Todas as atividades estão se acelerando profundamente. A informática, a cibernética, os novos equipamentos eletrônicos afetam as nossas percepções, alteram nossos hábitos, condicionando nossas decisões, pois passamos a ter uma ampla e complexa visão das consequências, ou seja, com as novas tecnologias precisamos tomar decisões mais rápidas, mas também mais complexas. Ao adotar uma tecnologia, é necessário decidir não somente sobre o desempenho organizacional, mas sobre quanto o trabalho humano será beneficiado, prejudicado ou mesmo eliminado e, consequentemente, o quanto será gerado de satisfação ou frustração entre os colaboradores (ALMEIDA, FREITAS e SOUZA, 2011)

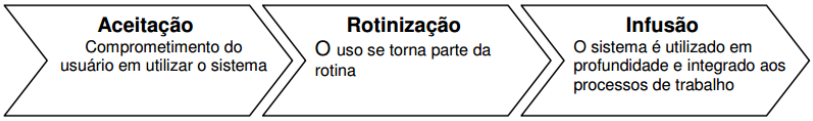
Santos (2007) coloca que a adoção de inovações em TI tem sido compreendida sob diferentes perspectivas, seja a: intenção de adoção, comportamento de adoção, uso real, decisão de adoção, processo decisório de adoção e difusão.

Molla e Licker (2005) comentam que a literatura de adoção de inovação apresenta algumas perspectivas dominantes, como: **gerencial, organizacional, tecnológica, ambiental e interacionismo**; onde esta última representa uma confluência entre as forças de inovação, bem como pode explicar diferenças marcantes no desempenho das organizações em situações contextuais idênticas.

Ao abordar o processo de adoção de inovações, Santos (2007) coloca que uma perspectiva gerencial baseia-se na característica inovadora do gestor, seu comprometimento com inovações e familiaridade com a TI; uma perspectiva organizacional considera que os direcionadores da adoção estão nas características internas da organização; a perspectiva tecnológica considera a complexidade, compatibilidade, vantagem relativa, facilidade de uso, utilidade percebida e outros atributos como condutores do processo de adoção; e a perspectiva ambiental tem foco nas influências externas, no mercado, na instituição, nas relações Inter organizacionais e forças socioeconômicas. Este autor baseia-se no modelo de Cooper e Zmud (1990) compreendido

em seis fases: iniciação, adoção, adaptação, aceitação, rotinização e infusão, onde discorre sobre as três últimas fases, conforme Figura 5.

**Figura 5: Processo de adoção e infusão**




Fonte: Santos, 2007

Santos (2007) apresenta algumas das principais teorias para adoção de TI, conforme Quadro 5 e conclui que os atributos percebidos da inovação, as características do sistema social, dos canais de comunicação, do tipo de decisão e dos esforços promocionais do agente de mudança são considerados fatores influenciadores da taxa de adoção.

**Quadro 5 – Principais teorias para adoção de TI**

| ***Teoria*** | ***Principais autores em TI/Ano*** | ***Análise nível individual*** | ***Análise nível organizacional*** |
|---|---|---|---|
| Teoria da Ação Racionalizada | Fishbein e Ajzen (1975) | X | |
| Teoria da Difusão da Inovação (DOI) | Rogers (1983, 1985) | X | X |
| Teoria Cognitiva Social | Bandura (1986) | X | |
| Modelo de Aceitação de Tecnologia (TAM) | Davis (1989) | X | |
| Teoria do Comportamento Planejado (TPB) | Ajzen (1991) | X | |
| Características Percebidas da Inovação | Moore e Benbasat | X | |
| Teoria Unificada de Aceitação e Uso de Tecnologia (UTAUT) | Venkatesh et al. (2003) | X | |
| Modelo de Difusão e Infusão | Kwon e Zmud(1987) | | X |

| | | | |
|---|---|---|---|
| Modelo "Tri-Core" de Inovação de SI | Swanson (1994) | | X |
| Teoria Ator-rede | Latour (2003) | X | X |
| Perspectiva Institucional | Teo, Wei e Bensbasat (2003) | | X |

Fonte: o autor

Molla e Licker (2005) concluem que vários dos modelos existentes de adoção destacam a relevância das limitações de infraestrutura tecnológica, financeira e legal, onde o estudo dos fatores de adoção de TI serve para destacar as limitações contextuais que muitas vezes são um dado adquirido em outros mercados. Concluem ainda que em alguns países, os recursos humanos e tecnológicos devem ser considerados na tomada de decisões de adoção, uma vez que o sucesso disso depende das mudanças organizacionais, nas características do produto e na cultura de negócio.

Rogers (2003) abordou em sua obra "*Diffusion of Innovations*", o processo de difusão e adoção de inovações e têm sido discutido por diversos autores.

Giacomini et.al. (2007) consideram a obra de Everett Rogers como uma das obras referenciais e, portanto, a analisam minuciosamente e concluem que existem lacunas (Quadro 6) no que concerne a atuais demandas sociais e comunicacionais atreladas ao tema. Afirmam que o conceito e o âmbito da difusão ou disseminação de inovações se confunde com o próprio processo da comunicação humana, uma vez que inovações, para serem socializadas, precisam ser difundidas. O modelo de Rogers, segundo estes autores, apresenta o fenômeno da inovação como algo sistêmico, privilegiando aspectos epistemológicos e tecnológicos das inovações.

**Quadro 6: Aspectos positivos e negativos da Teoria de Rogers, segundo Giacomini et.al. (2007)**

| ***Aspectos Positivos*** | ***Aspectos Negativos*** |
|---|---|
| O conceito de inovação utilizado por Rogers traz a questão do impacto social, uma vez que inovações quando não são percebidas como algo novo, tem suas propriedades inovadoras | Ao trazer a inovação relacionada a percepção, que estaria por sua vez, relacionada às teorias de aprendizagem, ou seja, um indivíduo ao perceber uma inovação, atribui-lhe um significado, |

| | |
|---|---|
| anuladas. | dentro de seu universo cognitivo. Mas Rogers não foca os interesses pessoais, culturais, políticos, ideológicos ou mercadológicos das inovações. |
| Mostra a legitimidade do marketing social na difusão de inovações, inclusive quando as inovações são impostas, onde enfatiza que muitas dessas ações inconvenientes para algumas pessoas, mas que são coagidas a adotar para o bem próprio e coletivo. | Não trata das inovações organizacionais em relação à realidade e desejo individual, nem trata do modelo cultural de países desenvolvidos sobre os demais países, ou seja, modelo de dominação. |
| Trata a difusão de inovações como algo processual e sistêmico, ou seja, Rogers se afasta da concepção de que uma inovação é algo pontual. | O estudo de Rogers não foca o universo cognitivo e sociocultural das pessoas, pois são os indivíduos que percebem e dão sentido a "novidade" e condicionam sua difusão. |
| Traz o conceito de "reinvenção", que seria o grau que uma inovação é mudada ou modificada por um usuário no processo de adoção e implementação. | Discute os atributos de inovações percebidos, mas atém-se a aspectos operacionais, como vantagens obtidas na adoção de uma inovação, compatibilidade com seus valores, complexidade para adotar a inovação, viabilidade e observabilidade em que os resultados são visíveis. |
| Traz a questão dos estudos de difusão de eventos noticiosos, que se difundem mais rapidamente que outras inovações, ou seja, o indivíduo precisa apenas obter conhecimento do evento noticiado, enquanto a adoção de inovações tecnológicas precisa de conhecimento, persuasão, decisão e implementação para seu processo decisório. Outra ressalva neste aspecto, é que Rogers não tece críticas sobre a cobertura jornalística de eventos políticos e bélicos. | Não discute obsolescência programada gerada por inovações, o impacto das constantes inovações para criar necessidades sociais supérfluas e gastos desnecessários, nem e as inovações que contrariam o movimento consumerista causando, inclusive, prejuízo são meio ambiente. |

Fonte: o Autor.

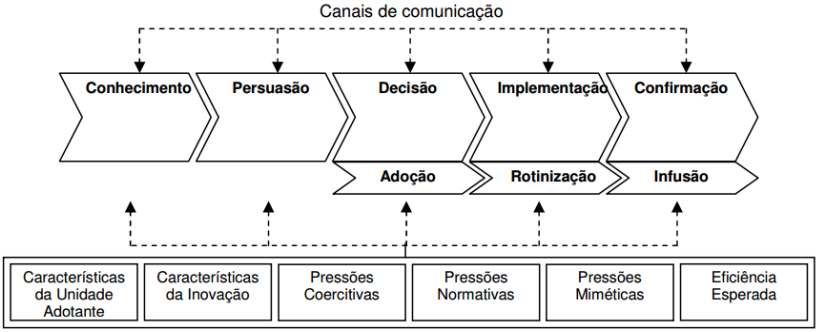
Em resumo, Giacomini et.al. (2007) discutem sobre o conceito de inovação dado por Rogers, que demandaria um foco intenso nas pessoas e nas relações sociais, como questões culturais, políticas e ideológicas,

que condicionam a forma como uma novidade é percebida, ou seja, levando em consideração a inovação servindo à sociedade.

Santos (2007) ao discutir a Teoria de Rogers comenta que o modelo falha ao considerar a inovação como resultado exclusivo de uma escolha estratégica, com base na eficiência de resultados, mostrando-se insuficiente para explicar situações onde a adoção ocorre por pressão política, poder ou outros fatores subjetivos que não sejam os de eficiência técnica.

Santos (2007) relaciona a teoria de Rogers (2003) com a de Cooper e Zmud (1990), adicionando características e pressões, além da adoção, rotinização e infusão, o que resultou no seguinte modelo (FIGURA 6):

**Figura 6: modelo proposto por Santos (2007)**




Fonte: Santos (2007)

Considera-se que uma inovação sempre envolve algo novo, com certo grau de incerteza em seu processo de adoção; inovações tecnológicas constituem fatores determinantes nas modificações sociais e econômicas; e que através de canais de comunicação as incertezas podem ser reduzidas (IGTI, 2013).

## 2.5 ANÁLISE DE IMPACTO

Quando se analisa a adoção de inovação em TI, pouco se questiona sobre o que ocorre após a decisão de adotar a inovação, resultando em uma lacuna a ser compreendida entre a adoção de uma inovação de TI e como esta é aceita e efetivamente utilizada, esta lacuna é denominada lacuna de assimilação; a maioria dos estudos sobre a adoção de inovação em TI utiliza como variável dependente a intenção de adoção (SANTOS, 2007).

Neste sentido, Bonacelli et al. (2003) comentam que a identificação, a quantificação e qualificação de impactos sociais de P&D é uma das vertentes mais importantes do processo de avaliação, por auxiliar a identificação da relação que se estabelece entre os resultados e atividades empreendidas por organizações envolvidas com pesquisa e as transformações percebidas por diferentes atores sociais.

Tigre (1998)coloca que existe hoje na literatura certo consenso sobre os impactos das inovações tecnológicas e organizacionais na estrutura da indústria e na organização das instituições, mas do ponto de vista da construção teórica, estes impactos não foram prontamente incorporados no pensamento econômico, onde o aporte de teorias oriundas de outras áreas do conhecimento permitia incorporar dimensões mais sutis e mais difíceis de serem captadas e incorporadas pelas teorias econômicas convencionais.

A identificação e a avaliação de tecnologias, sendo consideradas os primeiros passos no processo de P&D, combinam embasamentos para muitas das melhores práticas, onde a vantagem competitiva de longo prazo pode se derivar da estrutura e da cultura desenvolvidas por este processo de avaliação. (DAY; SCHOEMAKER; GUNTHER, 2003). Estes autores, ao estudarem o processo de mudança tecnológica, verificaram que tecnologias de primeira classificação *incrementaram* a taxa de melhoria no desempenho de produtos e variaram em dificuldade, do incremental ao radical, onde as empresas estabelecidas no setor tiveram a liderança no desenvolvimento e na adoção dessas tecnologias; já as inovações de segunda classificação *romperam* ou redefiniram as trajetórias de desempenho.

Diversos aspectos devem ser levados em consideração antes de se adotar ou não uma nova TI, tais como: descobrir tecnologias com potencial de oportunidade ou de perigo para a organização; avaliar a TI em relação à capacidade técnica da empresa, às necessidades do mercado alvo e às oportunidades de negócios que ela pode gerar; e, estudar os impactos financeiros, competitivos e organizacionais que a

adoção desta tecnologia pode causar à empresa. (MEDEIROS E SAUVÉ, 2003).

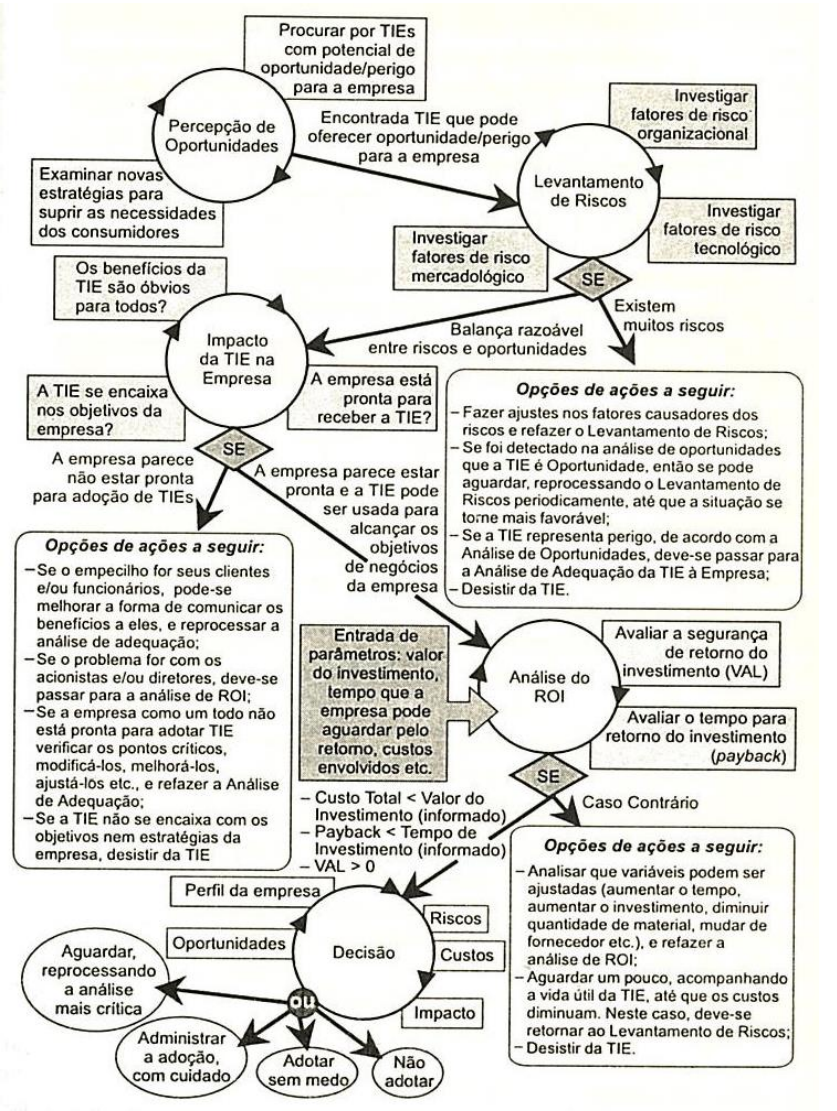
Marques (2008) coloca que uma das abordagens mais comuns para capturar impactos é a de caráter tecnocrático, que busca métodos científicos para auxiliar o encontro de uma abordagem ordenada e dedutiva, onde há um juízo de valor importante, pois se dá através do envolvimento de julgamento subjetivo de um especialista. Para tanto, apresenta etapas básicas do processo de avaliação de impacto: escopo (identifica os atores envolvidos); formulação de alternativas (baseadas nas necessidades dos atores); perfilhamento (descreve unidades e identifica indicadores); projeção (projeção do que é provável que aconteça e de quem será impactado, identificando indicadores, relações de causa-efeito e cenários); avaliação (determina magnitude, efeitos e impactos, ou seja, determina o potencial de mitigação); análise (benefícios, quem ganha, quem perde); mitigação (medidas para conter impactos não desejados); monitoramento (medida dos impactos pela observação); e auditoria pós-avaliação (checar a efetividade e o custo do estudo de impacto).

Medeiros e Sauvé (2003) apresentam o Processo para Avaliação de Impacto de Tecnologias da Informação Emergentes nas Empresas (FIGURA 7), que se configura em um gabarito de tomada de decisões. Está dividido em quatro etapas de análise, contendo 5 passos, que resumidamente são:

1. **Percepção de oportunidades:** avalia-se a tecnologia tentando retratá-la no futuro, suas incertezas, estratégias. As organizações devem estar constantemente atentas ao ciclo de vida das tecnologias importantes para seus negócios. Neste ponto podem ser utilizadas as seguintes metodologias: Análise de Cenários ou Análise de Opções Reais.
2. **Levantamento de Riscos:** são avaliados os riscos organizacionais, tecnológicos e mercadológicos, que podem ser analisados de *checklists*. Destaca-se que quando a TI é muito emergente, pode ser mais difícil avaliar os riscos mercadológicos relacionados com sua adoção. Outra questão importante, é que uma avaliação que indique um alto grau de risco tecnológico, pode ser vista como uma grande oportunidade de diferenciação, pois quanto mais emergente a TIE, mas chances de inovação a empresa pode ter investindo nela. Um dos métodos utilizados é o método de análise de risco.
3. **Impacto da TIE na empresa:** é preciso testar a adequabilidade da TIE à organização, analisar se ela está alinhada aos negócios/objetivos da organização e se as pessoas estão envolvidas com o processo de adoção. Este item também pode ser analisado através de um *checklist*.

4. **Análise do Retorno do Investimento (ROI):** nesta etapa, o resultado é obtido pela comparação entre os valores dos parâmetros informados pela empresa e o cálculo das variáveis financeiras de tempo de retorno, custo total e valor atual líquido do investimento.
5. **Decisão:** baseada nas oportunidades oferecidas, riscos avaliados e adequabilidade da tecnologia à organização, considerando custo-benefício, a organização pode decidir adotar, não adotar, aguardar ou adotar gradativamente a TIE.

**Figura 7 – Processo de Avaliação do Impacto de Tecnologias da Informação Emergentes nas organizações**




Fonte: Medeiros e Sauvé (2003, p.91)

Bonacelli et al. (2003) discorrem sobre a metodologia de avaliação de impactos de programas tecnológicos, que se baseia na identificação e mensuração *ex-post* da importância e intensidade de transformações de aspectos da realidade específicos e consequência do desenvolvimento, adoção e difusão de um programa de pesquisa, programa tecnológico ou de uma nova tecnologia. Esta metodologia faz "conversar" as diferentes dimensões e as percepções de diferentes atores envolvidos direta ou indiretamente. Os autores afirmam que as dimensões se configuram em recortes da realidade (componentes), ou seja, a estrutura de impactos funciona como uma rede cognitiva, que indica quais aspectos se deve considerar para examinar a extensão dos efeitos gerados.

Neste sentido, Maçada (2001) tratou, em sua tese de doutorado sobre o impacto dos investimentos em TI nas variáveis estratégicas e na eficiência dos bancos brasileiros, onde fez uma análise dos modelos de Mahmood e Soon (1991), que mede o impacto da TI nas variáveis estratégicas organizacionais em um contexto nacional; e de Palvia (1997), que utilizando a mesma estrutura formal do primeiro, avalia o efeito da TI em um contexto global. Ambos os modelos estão pautados na teoria da estratégia e competitividade, liderada por Porter (1980). De maneira genérica, esses modelos procuram identificar a capacidade da TI em alterar o modo das empresas operarem, de transformar a cadeia de valor e apoiar na implementação de estratégias (MAHMOOD e SOON, 1991 *apud* MAÇADA, 2001).

O modelo de Mahmood e Soon (1991) foi desenvolvido com o objetivo de identificar o impacto da TI nas variáveis estratégicas das organizações, sendo composto por 10 dimensões estratégicas, conforme Quadro 7:

**Quadro 7 - Dimensões do modelo de Maçada e Soon (1991)**

| Dimensão | Conceito |
|---|---|
| Clientes | A TI pode beneficiar os clientes das organizações, disponibilizando informações sobre produtos e serviços, e oferecendo suporte administrativo como cobrança, controle de saldos de conta, entre outros. |
| Competitividade | A TI pode aumentar, de várias maneiras, a posição competitiva da organização, com relação a seus concorrentes, tais como: diferenciando seus produtos e serviços, oferecendo algo que seus competidores não |

| | |
|---|---|
| | podem oferecer, oferecendo produtos e serviços substitutos antes dos competidores e estabelecendo nichos de mercado. |
| Fornecedores | A TI pode aumentar o poder sobre os fornecedores. As organizações podem utilizar a TI como ferramenta capaz de monitorar e identificar os fornecedores de recursos, além de buscar fontes alternativas de recursos. |
| Custos de coleta e troca | Todos os usuários de TI enfrentam custos de troca. Se a organização está tentando penetrar no mercado, ou introduzir uma nova tecnologia de informação na obtenção de competitividades, não deve ignorar os custos que os clientes têm de arcar para mudar para seus produtos, serviços e informações. Esse constructo inclui o tempo e os gastos para procurar e investigar novos fornecedores, assegurar ganhos de qualidade e menor tempo de entrega, negociar contratos e buscar informações para dar suporte ao processo decisório. |
| Mercado | Sistemas de informação de marketing tais como, *database* marketing, *data warehouse* e *data mining* podem ajudar as organizações a formar uma forte vantagem competitiva perante seus concorrentes. Os benefícios desses sistemas não só incluem o desempenho das funções de marketing tradicional, mas também fornecem acesso direto a mercados remotos e possibilitam altas demandas sobre produtos e serviços com base na TI, especificamente através dos recursos da internet e das aplicações de comércio eletrônico. |
| Produtos e serviços | A TI permite modificar a natureza de produtos e serviços das organizações, pela diminuição dos seus ciclos de vida, acentuando seus valores e desempenhos, melhorando a qualidade e fornecendo informações e conteúdo para os clientes. |
| Estrutura de custos e capacidade | Altos investimentos em automação e na tecnologia Internet (ex.: comércio eletrônico) podem reduzir o custo por unidade de produção, obter economias de escala pela utilização de maquinário, espaço, energia e trabalho especializado mais eficientemente e melhorar o equilíbrio existente entre padronização e flexibilização dos processos nas organizações. |
| Eficiência organizacional interna | Diversos tipos de TI (ex.: videoconferência, e-mail) tem sido comumente utilizados pelas organizações para tornarem as comunicações mais rápidas, convenientes e confiáveis. Através da TI, as organizações podem monitorar e coordenar mais de perto as atividades |

| | |
|---|---|
| | realizadas pelas firmas, pelos seus compradores e fornecedores, e expandir seus mercados ou negócios, em nível doméstico ou internacional. |
| Eficiência interoganizacional | Através do uso da TI (ex.: sistemas de apoio à decisão), o processo de tomada de decisão pode ser simplificado. Uma melhor coordenação entre as áreas funcionais pode ser realizada. Em uma organização de prestação de serviços, qualquer sistema computadorizado, apoiado em TI, pode auxiliar na redução do tempo de atendimento e consequentemente diminuir o *back-log* (fila). Com alta eficiência interna, a organização encontra benefícios, como altas margens de lucro e divisão de mercado. |
| Preços | A TI pode auxiliar a tornar mais oportuna a mudança de preços e melhorar a formulação de preços, além disso, ajudar no processo de formação de preços, disponibilizando informações importantes como custo do produto, dados de mercado, entre outros. |

Fonte: IGTI (2013).

Angeloni (2002) coloca que sempre que se pretende sugerir um modelo teórico acerca de um fenômeno social complexo, devem-se considerar as limitações acerca das percepções de quem o concebe, bem como as simplificações incapazes de explicar o todo. Esta autora, utiliza três dimensões em seu modelo teórico de organizações de conhecimento: **dimensão infraestrutura organizacional** (visão holística, estilo gerencial, cultura organizacional, estrutura organizacional flexível – é a dimensão que contém os elementos responsáveis pela existência e manutenção da totalidade e da continuidade da organização); **dimensão pessoas** (integração de diversos níveis de conhecimento e de expressão, ação coordenada e desenvolvimento de habilidades); e **dimensão tecnológica** (computadores, redes e softwares).

Desta forma, no que diz respeito ao dimensionamento, adota-se as definições das dimensões da sustentabilidade, utilizadas por Mendes (2009), o qual se baseou em Sachs (1993), uma vez que nesta concepção, julga-se adotar as principais relações da sociedade: ecológica; cultural; econômica, política; social e territorial, onde foi adicionada à dimensão tecnológica, foco deste estudo, conforme Quadro 8:

**Quadro 8: Definição das dimensões de análise, baseado em Mendes (2009) Angeloni (2002) e Marques (2008)**

| Dimensão | Definição |
|---|---|
| Ambiental/ecológica | Preservação dos recursos naturais na produção de recursos renováveis e na limitação de uso dos recursos não-renováveis; limitação do consumo de combustíveis fósseis e de outros recursos esgotáveis ou ambientalmente prejudiciais, substituindo-os por recursos renováveis e inofensivos; redução do volume de resíduos e de poluição, por meio de conservação e reciclagem; autolimitação do consumo material; utilização de tecnologias limpas; definição de regras para proteção ambiental. |
| Cultural | Diz respeito à cultura de cada local; garantindo continuidade e equilíbrio entre a tradição e a inovação. |
| Econômica | Eficácia econômica avaliada em termos macrossociais e não apenas na lucratividade empresarial, desenvolvimento econômico intersetorial equilibrado; capacidade de modernização contínua dos instrumentos de produção; razoável nível de autonomia na pesquisa científica e tecnológica; inserção soberana na economia internacional.<br>É possibilitada por alocação e gestão mais efetivas dos recursos e por um fluxo regular do investimento público e privado nos quais a eficiência econômica deve ser avaliada com o objetivo de diminuir a dicotomia entre os critérios microeconômicos e macroeconômicos. |
| Política | No âmbito nacional baseia-se na democracia, apropriação universal dos direitos humanos; desenvolvimento da capacidade do Estado para implementar o projeto nacional em parceria com empreendedores e em coesão social. No aspecto internacional tem sua eficácia na prevenção de guerras, na garantia da paz e na promoção da cooperação internacional e na aplicação do princípio da precaução na gestão do meio ambiente e dos recursos naturais; prevenção da biodiversidade e da diversidade cultural; gestão do patrimônio global como herança da humanidade; cooperação científica e tecnológica internacional. |
| Social | Abrange a necessidade de recursos materiais e não-materiais, objetivando maior equidade na distribuição da renda, de modo a melhorar substancialmente os direitos e as condições da população, reduzindo-se o |

| | |
|---|---|
| | índice de GINI [2], ampliando-se a homogeneidade social; a possibilidade de um emprego que assegure qualidade de vida e igualdade no acesso aos recursos e serviços sociais. |
| Tecnológica | Recursos de *hardware* e *softwares* são ferramentas que estão sendo disponibilizadas para criar, armazenar, resgatar e distribuir conhecimentos, ou seja, apoiam a tomada de decisão e o gerenciamento de informações e conhecimento. As organizações necessitam utilizar recursos tecnológicos para gerenciar seu conhecimento acumulado e em desenvolvimento. A novidade tecnológica contribui para o desenvolvimento de novos produtos ao possibilitar modificações na forma, desempenho, custo e parâmetros de um produto, alterando ainda o desempenho dos meios de produção e dos insumos. |
| Territorial | Busca de equilíbrio na configuração rural-urbana e melhor distribuição territorial dos assentamentos humanos e atividades econômicas; melhorias no ambiente urbano; superação das disparidades inter-regionais e elaboração de estratégias ambientalmente seguras para áreas ecologicamente frágeis a fim de garantir a conservação da biodiversidade e do ecodesenvolvimento. |

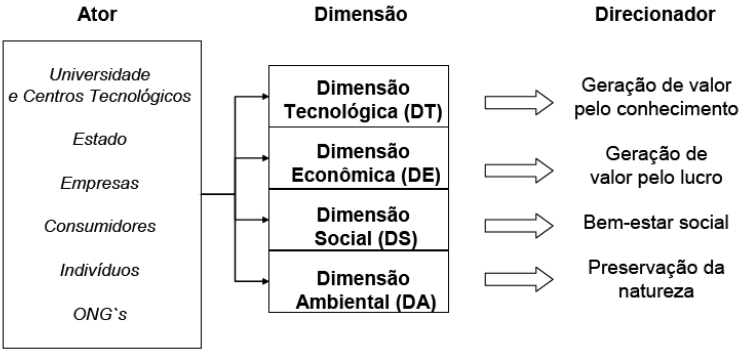
Fonte: baseado em Mendes (2009),Angeloni (2002) e Marques (2008)

Marques (2008) em sua tese aborda o contexto econômico que envolve novas tecnologias; defende a ideia de que estas novas tecnologias impactam não só a economia, mas a sociedade e o meio-ambiente, e, portanto, defende a ideia de que existem relações entre as dimensões, e que estas relações podem ser simultâneas. Comenta ainda que, quando os impactos são muito intensos, como no caso de tecnologias revolucionárias, eles tendem a se propagar para outras dimensões, como a social e a ambiental. Este autor coloca que na dimensão econômica o impacto pode implicar tanto no aumento da produtividade e o crescimento da riqueza, como também no desaparecimento de setores econômicos, dentre outras questões. Já a dimensão social diz respeito às normas e restrições impostas pela sociedade. E, por fim, a dimensão ambiental, está relacionada ao conceito de sustentabilidade, ou seja, a aplicação racional dos recursos naturais. A Figura 8 demonstra de forma sucinta as relações entre dimensões e direcionadores do modelo de Marques.

Marques (2008) ao desenvolver seu modelo coloca que os impactos são resultados das ações de determinados atores (ou agentes)(sejam grupos ou indivíduos que influenciam ou são influenciados) que possuem papéis específicos em cada dimensão, portanto, agrupou ações com propósitos semelhantes na forma de dimensões espaciais, que funcionam como fronteiras de relações dinâmicas estabelecidas tanto internamente (intradimensional) quanto com as demais dimensões (interdimensional), ou seja, identificou um conjunto de relacionamentos a partir das ações dos atores, que reflete diretamente no tipo de impacto gerado e defende a ideia de que todos os sentidos de relacionamento devem ser considerados na avaliação de impacto de uma nova tecnologia e que pela lógica o ponto de início dos relacionamentos deve partir da dimensão tecnológica, por se tratar da análise de uma nova tecnologia.

Marques (2008) destaca que cada impacto tem a capacidade de gerir ou contribuir com novos impactos na própria dimensão ou nas demais dimensões.

**Figura 8: Relação entre atores, dimensões e direcionadores do modelo**




Fonte: Marques (2008, p.54)

Os direcionadores do modelo de Marques (2008) representam as interações entre as dimensões, que são definidas por ele como modo de desenvolvimento, por exemplo, as interações entre as dimensões tecnológica e econômica têm como elemento que estrutura estas relações entre seus atores, o regime de acumulação de capital, já as relações entre as dimensões tecnológica, econômica e social, apresentam um ou mais modos de regulação (marcos regulatórios) instituídos por meio das formas institucionais.

## 2.6 VISÃO SISTÊMICA DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Considerando a certificação digital como a mais nova realidade na identificação pessoal e nas transações *online*, torna-se relevante entender como sua adoção e seu uso impactam a vida dos cidadãos e das organizações, a fim de que se possa pensar, prospectar e planejar à longo prazo as questões de segurança de informação. Para que isso possa ser realizado, é preciso entender o sistema que regula a certificação digital, que no caso do Brasil é a Infraestrutura de Chaves Pública Brasileira (ICP-Brasil). Pensar, "olhar" e agir sistematicamente, permitem a identificação e o entendimento de vários fatores envolvidos no sistema de certificação (VALCARENGHI et.al. 2013)

A análise da ICP-Brasil, estrutura responsável pela viabilização da emissão de certificados digitais para identificação virtual do cidadão e organizações, baseada na Teoria Geral dos Sistemas, que será realizada no decorrer deste item, permitirá conhecer e entender as relações, os componentes e suas partes. A análise minuciosa das partes deste sistema permite que, a partir de sua observação, seja criada uma visão capaz de demonstrar um diagnóstico, que proporcione uma gama de possibilidades de elaboração de propostas de melhorias e um efetivo processo de tomada de decisão, ou seja, que permita de forma estruturada, prospectar cenários de futuro da certificação digital no Brasil, bem como entender os impactos gerados no momento de sua adoção.

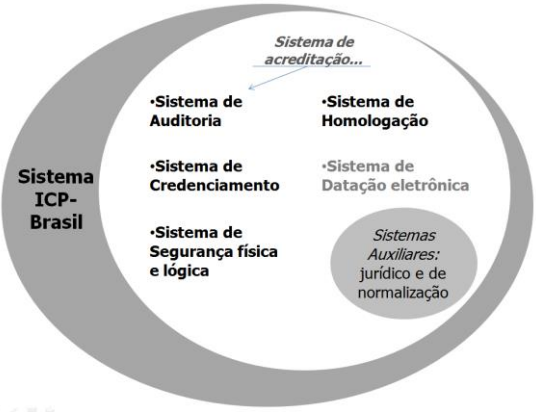
Esta abordagem fornece uma visão de alto nível de qualquer tipo de sistema, identificando os componentes, os elementos externos com os quais interagem os componentes (ambiente), a estrutura de ligações entre os componentes e destes com o ambiente, e os mecanismos que determinam o comportamento do sistema (MALDONADO E COSER, 2010).

A partir do referencial teórico estudado, pode-se considerar o sistema ICP-Brasil, como um sistema teleológico (*top-down*), aberto, cabendo analisar seus componentes e relações.

Ao abordar a ICP-Brasil como um sistema, Martini (2008) coloca que a certificação digital ICP-Brasil é suportada pelo Sistema Nacional de Certificação Digital, como um sistema composto de subsistemas fundamentais e construtivos, conhecido por ICP-Brasil, o qual, é composto por diversos subsistemas como: i) Subsistema de acreditação – que visa a auditoria de conformidades aos padrões de interoperabilidade e de segurança das ACs e ARs integrantes e seu

credenciamento; ii) Subsistema de Segurança Física e lógica – um sistema rigoroso e exigente para ambientes computacionais; iii) Subsistema de homologação de sistemas e equipamentos – para homologação de sistemas e equipamentos – Laboratório de Ensaios e Auditoria (LEA); iv) Subsistema de datação eletrônica; v) Subsistema Jurídico e de Normatização – um sistema auxiliar para dar tratamento público e bem definido às regras do sistema ICP-Brasil; conforme Figura 9.

**Figura 9: Sistema ICP-Brasil e seus subsistemas, segundo Martini (2008)**




Fonte: Martini (2008, p. 36).

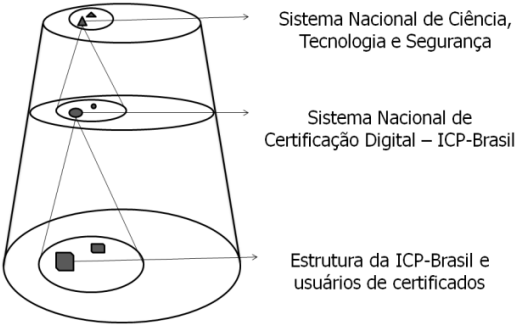
Como atores do sistema ICP-Brasil, Martini coloca: organizações (públicas e privadas), profissionais liberais e o cidadão, os quais estão inter-relacionados e apresentam interesses e expectativas distintas. Assim, a ICP-Brasil se define como um ambiente dinâmico e complexo que transcende a questão puramente tecnológica e envolve questões culturais, sociais, econômicas e até ambientais. Os principais atores envolvidos na ICP-Brasil podem ser elencados como: a Diretoria de Auditoria, Fiscalização e Normalização (DAFN/ITI), Diretoria de Infraestrutura de Chaves Públicas (DINFRA/ITI), Procuradoria Federal Especializada (PFE/ITI), Laboratório de Ensaios e Auditoria, Escritórios de Auditoria Independente, Autoridades Certificadoras, Autoridades de Registro e usuários (pessoas físicas e jurídicas).

O sistema ICP-Brasil pode ser definido como um sistema aberto de origem teleológica. Aberto, pois realiza interações entre as partes e teleológico, por ter sido projetado e construído com uma finalidade previamente definida. Isso implica categorizá-lo como um sistema "*Top-*

*Down*". Parte-se do supersistema imediatamente acima dele e acaba por criar subsistemas, que juntos o constituem. Essa representação de sistema em níveis pode crescer indefinidamente, mas de modo geral trabalha-se com três níveis devido a complexidade da análise (VALCARENGHI et.al. 2013).

Adota-se nesta pesquisa a representação hierárquica de sistemas, onde o sistema e seus componentes são abordados em três diferentes níveis: 1 - nível de supersistema, 2 - sistema e de 3 – subsistema, conforme Figura 10.

**Figura 10: Níveis hierárquicos do Sistema Nacional de Segurança e Tecnologia - sistema teleológico**




Fonte: VALCARENGHI et.al. 2013.

A figura acima, segundo seus autores, representa a ICP-Brasil em seus três níveis: 1) **nível macro ou suprasistema**: o Sistema Nacional de Ciência, Tecnologia e Segurança (configurado pelo Ministério de Ciência, Tecnologia e Inovação – MCTI, Ministério de Comunicações – MC, Ministério de Defesa - MD, Casa Civil - CC, e Gabinete de Segurança Institucional - GSI); 2) **nível de sistema**: o Sistema Nacional de Certificação Digital, representado pela ICP-Brasil; e 3) **nível de subsistemas**: as entidades e atores que compõem a ICP-Brasil (Comitê Gestor, AC-Raiz, AC de 1º nível, AC de 2º nível, AR) e suas relações (órgãos públicos, órgãos privados, empresas, cidadão). Da mesma forma, ao analisá-la considerando a ICP-Brasil como sistema, do ponto de vista de sua hierarquia organizacional, obtém-se a seguinte representação (Figura 11):

**Figura 11: Níveis hierárquicos da ICP-Brasil - do ponto de vista de sua hierarquia organizacional**


Fonte: VALCARENGHI et.al. 2013.

Do ponto de vista interno, a ICP-Brasil é composta por diversos sistemas, como representado na Figura 12:

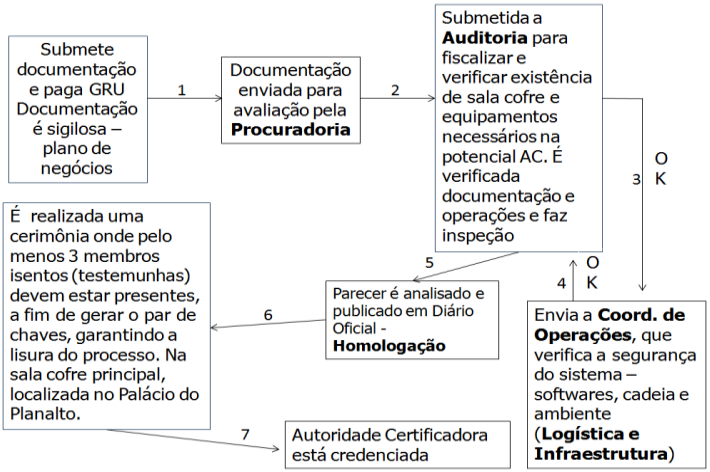
**Figura 12: Níveis da ICP-Brasil – do ponto de vista interno**


Fonte: VALCARENGHI et.al. 2013

Segundo Valcarenghi et.al. (2013) para se entender como os subsistemas dentro da ICP-Brasil se comportam, é necessário o

entendimento dos processos envolvidos, citando como exemplo o processo de credenciamento de uma AC (Figura 13):

**Figura 13: Representação dos processos de credenciamento de uma AC**




Fonte: VALCARENGHI et.al. 2013.

Sendo um sistema uma construção mental produzida pelo observador, onde está presente uma coleção de objetos inter-relacionados em uma dada estrutura totalizando o todo, sendo que uma dada funcionalidade o identifica como tal, Alves (2012) afirma que o Estado do sistema, pode ser tratado como a condição na qual um sistema se encontra em determinado momento e que é definido a partir das variáveis do sistema definidas pelo observador. Diante disso, no sistema em questão, a definição de variáveis para a avaliação dos processos e determinação de estados é de suma importância. Essas variáveis do sistema podem ser consideradas como indicadores capazes de subsidiar tomadas de decisões. (VALCARENGHI et.al. 2013)

Bunge (2003) ao tratar de sistemas afirma que qualquer sistema pode ser modelado segundo a quádrupla: *Composition – Environment – Structure – Mechanism* – ou modelo CESM, onde: **composição** é uma coleção de todas as partes do sistema ou elementos componentes; **ambiente** é uma coleção de itens que não pertencem ao sistema, mas atuam ou sofrem a ação por algum ou todos os componentes do sistema; **estrutura** é uma coleção de ligações entre componentes e entre esses itens do ambiente; e **mecanismo** é uma coleção de processos que fazem o sistema se comportar da maneira que tem de se comportar.

O Quadro 9 representa o modelo sociotécnico de Bunge (2003) aplicado na ICP-Brasil.

**Quadro 9: Sistema sociotécnico da ICP-Brasil baseado no modelo CESM**

| | |
|---|---|
| **COMPOSIÇÃO**<br>**(partes do sistema)** | - Comitê Gestor,<br>- Instituto Nacional de Tecnologia de Informação – ITI, como AC-Raiz (sistema jurídico, sistema de auditoria, sistema de logística e infraestrutura, sistema de homologação, e credenciamento)<br>- AC de 1º nível<br>- AC de 2º nível<br>- Autoridade de Registro<br>- Profissionais que atuam nestas instituições<br>- Tecnologias da Informação e Comunicação – TICs, etc.<br>-Portador de certificado digital (cidadão, organizações públicas e privadas) |
| **AMBIENTE**<br>**(itens que não pertencem ao sistema, mas atuam ou sofrem a ação por algum ou todos os seus componentes)** | Pessoas ou organizações públicas e privadas que não possuem certificado. |
| **ESTRUTURA**<br>**(ligações entre componentes e entre esses e itens do ambiente)** | - Normatização;<br>- Agendamento;<br>- Atendimento<br>- Emissão de Certificados (certificados de AC e AR, certificados de atributos, etc);<br>- Instalação<br>- Monitoramento<br>- Renovação<br>- Revogação<br>- Fiscalização<br>- Auditoria, etc. |
| **MECANISMO**<br>**(processos que fazem o sistema se comportar da forma que tem de se comportar)** | - Cadeia de Confiança |

Fonte: VALCARENGHI et.al. 2013.

Para Valcarenghi et.al. (2013) a análise da ICP-Brasil a partir do modelo CESM permitiu a compreensão dos atores do sistema (**composição**); bem como o **ambiente** onde a ICP-Brasil está inserida; sua **estrutura**, onde se apresentam as relações entre componentes e ambiente; o **mecanismo**, onde neste caso se configura sua razão de existir; e a fronteira, que neste caso são os portadores de certificado digital, sejam eles AC's, AR's, empresas públicas ou privadas, ou usuários finais e concluem que não foi identificado o processo de monitoração deste sistema.

## 2.7 CONSIDERAÇÕES PERTINENTES À REVISÃO DA LITERATURA

Em resumo, procurou-se levantar algumas questões a respeito da sociedade do conhecimento e das Tecnologias de Informação e Comunicação, que refletissem a necessidade de se pensar em tecnologias de segurança da informação e do conhecimento, a fim de inserir a certificação digital neste contexto.

Posteriormente, apresentou-se a Infraestrutura de Chaves Públicas e questões de criptografia e emissão de certificado digital, além de aspectos gerais que envolvem certificação digital, as publicações acadêmicas no Brasil e algumas aplicações, onde percebeu-se a necessidade de se analisarem alguns modelos de adoção de inovações tecnológicas, uma vez que a literatura demonstra que técnicas de difusão e de adoção escolhidas por gestores e organizações, podem refletir no impacto de adoção e uso desta tecnologia.

Procurou-se ainda entender o processo de análise de impacto, onde a teoria permitiu identificar as dimensões a serem analisadas nesta pesquisa, a fim de realizar uma análise multidimensional da tecnologia escolhida.

Por fim, foi realizada uma análise da Certificação digital ICP-Brasil sob a visão sistêmica, onde, como sistema complexo, em que diversos outros sistemas estão envolvidos, considera-se que outras análises devem ser feitas a fim de aprofundar o entendimento destes sistemas que estão direta ou indiretamente envolvidos ou que interferem seja na existência, estrutura, funcionamento, relacionamentos da ICP, dentre outras questões.

Desta forma, a partir do entendimento da ICP-Brasil sob uma visão sistêmica, a próxima etapa desta pesquisa retoma à identificação das dimensões selecionadas na revisão de literatura e identificação de alguns questionamentos relacionados a impacto, identificados na revisão de literatura, a fim de construir o roteiro das entrevistas, como será detalhado na próxima seção.

Em resumo, esta pesquisa utilizou-se das teorias de Mendes (2009), Angeloni (2002) e Marques (2008) para identificar e descrever as dimensões utilizadas nesta pesquisa e a teoria de Bunge (2003) para análise sistêmica.

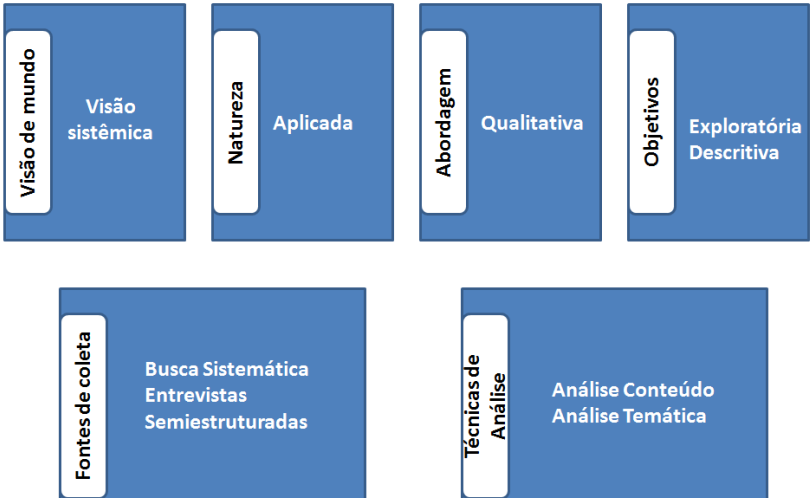
## 3. PROCEDIMENTOS METODOLÓGICOS

Neste capítulo é descrito o caminho metodológico que direciona o alcance dos objetivos propostos nesta pesquisa. Segundo Gil (2008) o método científico possibilita identificar operações mentais e técnicas que possibilitem a verificação de um conhecimento, ou seja, é o caminho para se chegar a determinado fim. Este autor classifica os métodos em dois grandes grupos: 1) os que proporcionam bases lógicas de investigação científica (dedutivo, indutivo, hipotético dedutivo, dialético, ou fenomenológico) e 2) os que esclarecem acerca dos procedimentos técnicos que podem ser utilizados (experimental, observacional, comparativo, estatístico, clínico, ou monográfico).

Trata-se de um recorte do macroprojeto intitulado "Avaliação de impacto socioeconômico da certificação digital no Brasil", firmado por meio de Termo de Cooperação Nº 02/2012 entre o Instituto Nacional de Tecnologia da Informação – ITI e a Universidade Federal de Santa Catarina – UFSC, por meio do Núcleo de Estudos em Inovação, Gestão e Tecnologia da Informação (IGTI/UFSC), aprovado pelo Comitê de Ética em Pesquisa da Universidade Federal de Santa Catarina – UFSC.

Desta forma, as seguintes etapas, apresentadas na Figura 14, representam o modelo que define os procedimentos metodológicos que foram utilizados para a construção desta pesquisa.

**Figura 14: Abordagem metodológica da pesquisa**




Fonte: o Autor.

## 3.1 CARACTERIZAÇÃO DA PESQUISA

Quanto à caracterização, esta pesquisa será analisada a partir de sua visão de mundo/paradigma, onde adotou-se a **visão sistêmica** ou teoria bunguiana; quanto à sua abordagem configura-se como uma pesquisa **qualitativa**; quanto à sua natureza, configura-se como uma pesquisa **aplicada**; quanto aos objetivos, configura-se como uma pesquisa **exploratória descritiva**; e procedimentos técnicos utilizados.

### 3.1.1 Quanto à visão de mundo

Entende-se que este trabalho enquadra-se na Teoria Geral dos Sistemas– TGS, tendo como um dos pioneiros o autor Ludwig von Bertalanffy (1967), uma vez que seu conteúdo é a formulação e derivação dos princípios válidos para os "sistemas" em geral, tendo como consequência o aparecimento de semelhanças estruturais ou isomorfismos em diferentes campos, ou seja:

> [...] se definirmos de modo conveniente o conceito de sistema, verificaremos que existem modelos, princípios e leis que se aplicam aos sistemas generalizados qualquer que seja seu tipo particular e os elementos e "forças" implicadas (Bertalanffy, p.57, 2010).

Vasconcelos (2002) ao tratar da teoria de Bertalanffy, coloca que ele se dedicou a identificar princípios básicos interdisciplinares que pudessem constituir uma teoria interdisciplinar, uma teoria de princípios universais, algo que influência nossa visão de mundo, ou seja, a TGS "se propõe como uma ciência da totalidade, ou como uma disciplina lógico-matemática aplicável a todas as ciências que tratam de "todos organizados" (VASCONCELOS, 2002, p.196). Vasconcelos ainda coloca que é uma ciência voltada para um mundo dinâmico e fundamentada no conceito de interação e objetividade, onde há "perspectivas da realidade".

A TGS se colocou como uma teoria de princípios universais aplicáveis aos sistemas em geral, sejam de natureza física, biológica ou sociológica; desenvolvendo os princípios básicos interdisciplinares. (VASCONCELOS, 2002)

Chiavenato (2003), por sua vez, aponta que a TGS estuda os sistemas globalmente, buscando identificar todas as interdependências de suas partes. Ainda apresenta a TGS como fundamentada em três

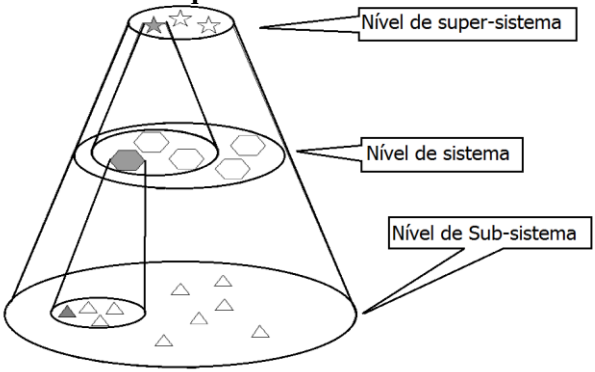
premissas básicas: a) sistemas existem dentro de sistemas, sendo cada sistema composto por subsistemas e fazem parte de um sistema maior, o qual é denominado suprasistema; b) sistemas são abertos, ou seja, possuem um processo infinito de intercâmbio com seu ambiente; e a última premissa é c) que as funções de um sistema dependem de sua estrutura. Outra contribuição importante que este autor traz, é que o conceito de sistema proporciona uma visão compreensiva, abrangente, holística e gestáltica de um conjunto de coisas complexas dando-lhes configuração e identidade.

Compreende-se por sistema o conjunto de partes interagentes e interdependentes, que formam um todo unitário com determinado objetivo e que efetuam determinada função. Estes sistemas são compostos de subsistemas e supra sistemas, sendo fechados ou abertos, apresentando entropia positiva ou negativa, como será visto no decorrer deste trabalho (ALMEIDA, FREITAS e SOUZA (2011).

A habilidade de se observar e compreender um sistema em seu todo, analisando suas partes e as relações entre elas, ou seja, compreender que o todo é maior do que a soma das partes, é denominada visão sistêmica, ou teoria Bunguiana, que segundo Pietrocola (1999), busca efetuar a vinculação de modelos filosóficos, com a realidade ontológica associada ao mundo físico. Em outras palavras, propõe que um sistema não existe por si só, que não é possível sua compreensão por completo e que ele está inserido em um ambiente com o qual efetua trocas, sejam elas diretas ou não.

Alves (2012) coloca que todo ser humano é dotado de uma visão de mundo própria, individual e única, construída ao longo de sua história. Ao viver em sociedade, torna-se necessária uma visão de mundo coletiva, denominada paradigma. Neste sentido, a visão sistêmica permite que, a partir da construção mental de um sistema, torna-se necessário sintetizá-lo ou resumi-lo. Descrevendo seus componentes e suas relações, e pelo menos uma funcionalidade. Desta forma, o autor apresenta a representação hierárquica de sistema, de forma a elucidar simplificadamente a hierarquia existente entre os componentes e o sistema que formam (Figura 15). Para tanto, divide o sistema a ser analisado em três níveis: 1) nível de supersistema; 2) nível de sistema; e 3) nível de subsistema. Podendo estar subdividido, em princípio, ilimitadamente, mas aconselha abordar apenas três, a fim de evitar-se dispersão analítica.

**Figura 15: Níveis hierárquicos de sistemas**




Fonte: Alves, 2006

Fernandes (2012) coloca que o emprego da visão sistêmica à concepção de sistemas se justifica pelo fato de que esta visão torna perceptível o movimento integrado entre o ambiente, nossas decisões e o futuro. Em resumo, pode-se considerar um exercício de percepção.

Vasconcelos (2002) traz a ideia do pensamento sistêmico como novo paradigma da ciência, como visão, como pressuposto epistemológico.

Bonacelli et al. (2003) ao tratarem do processo de avaliação de P&D, colocam que captar a amplitude dos resultados e impactos gerados pela produção e incorporação de conhecimento, significa considerar a complexidade de um sistema de pesquisa científica e tecnológica, e ainda as interações existentes entre este sistema mais amplo e complexo.

Ao se analisar se um sistema é fechado ou aberto, Almeida, Freitas e Souza (2011) colocam que um sistema fechado é aquele que não sofre intervenções externas, ou seja, dificilmente exista um sistema fechado em sua forma pura.

Quando se trata de visão sistêmica é preciso considerar a existência de um observador, um fator de grande influência na análise do sistema, ou seja, qualquer alteração no sistema, pode provocar alterações tanto no ambiente, quanto na visão de mundo deste observador. Segundo essa lógica, a soma da visão de mundo de vários observadores não necessariamente definirá com perfeição o mundo real (MATURANA E VARELA, 2004)

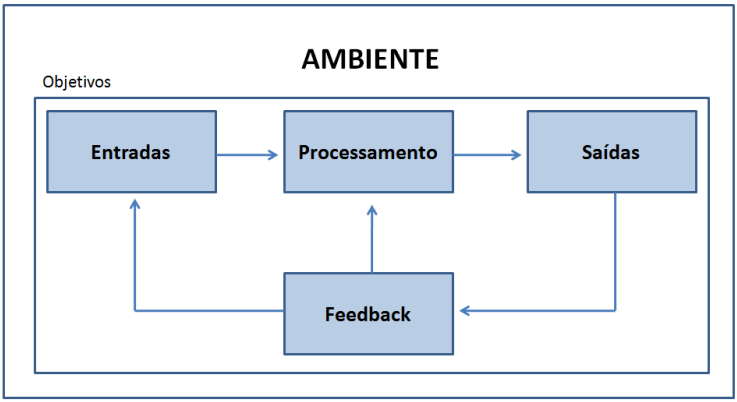
Em relação a construção de sistemas, diz-se que um sistema é denominado teleológico ou *top-down*, quando foi projetado e construído com uma finalidade, concebido para cumprir um objetivo. Um sistema

pode configurar sistemas diferentes, dependendo da aferição das variáveis consideradas por cada observador, neste sentido, cada sistema está inserido em um ambiente, o que significa que há uma fronteira, ou seja, há algo que caracteriza uma separação entre eles, o que os diferencia. Há uma correlação direta entre observador e fronteira. A fronteira delimitadora faz parte intrínseca do sistema e tem grande importância, sendo ela o determinante se o sistema pode ou não trocar informação/energia com o ambiente. Em um sistema fechado, criado a partir de uma fronteira fechada, sua entropia tende a crescer, levando o sistema ao colapso (ALVES, 2012).

Alves (2012) trata em sua obra do processo de monitoração e controle de sistemas, onde coloca que o sistema construído mentalmente pelo observador contém apenas os aspectos mais relevantes do fenômeno em si, o que reduz sua complexidade a níveis que permite a monitoração e o controle, sendo que esta monitoração tem por objetivo acompanhar a situação (estado) em que o sistema se encontra ao longo do tempo, ou seja, não há como controlar algo que não se consegue monitorar.

Neste mesmo sentido, como todo sistema tem um insumo, que passa por um processamento, gerando saídas ou resultados esperados, ou seja, é o objetivo do sistema, para que alcance os resultados esperados, o sistema deve ser constantemente avaliado, por meio de *feedback* ou retroalimentação, conforme Figura 16 (ALMEIDA, FREITAS E SOUZA, 2011).

**Figura 16: Esquema conceitual de um sistema**



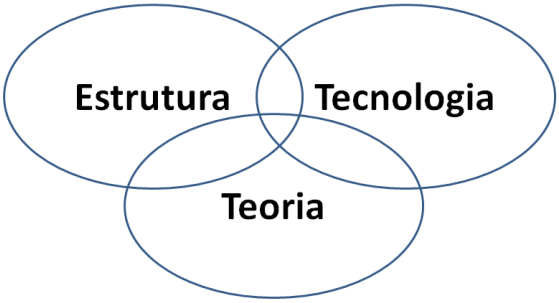

Fonte: Almeida, Freitas e Souza (2011).

A Figura 16, mostra que o *feedback* influencia tanto nas entradas, como no próprio processamento, ou seja, os resultados observados devem ser mensurados frente aos objetivos e as causas de distorções devem ser identificadas e eliminadas para que o sistema funcione com perfeição.

Outra questão que concerne aos sistemas é a entropia. Em geral, os sistemas têm entropia positiva, o que significa que eles têm uma tendência à desordem e à destruição. É preciso manter e fortalecer o sistema através da entropia negativa ou homeostase, ou seja, mantê-lo em equilíbrio, para que possa resistir ao longo do tempo; de forma flexível, criativa e inovadora, enxergando o todo e as partes (ALMEIDA, FREITAS e SOUZA, 2011).

Ao tratar de sistema social, Angeloni (2002) coloca que todo ele é um sistema epistemológico, ou seja, um mecanismo de produção e reprodução de conhecimento, onde toda organização social é um sistema de aprendizagem, e aponta o modelo de organização de Schon (1971), que considera que todo sistema social (Figura 17) é constituído por uma estrutura (relações estabelecidas), uma tecnologia (conjunto de normas, ferramentas e técnicas) e uma teoria (conjunto de regras epistemológicas por meio das quais se interpreta a realidade).

**Figura 17: Dimensões dos sistemas sociais**




Fonte: Angeloni (2002).

Angeloni (2002) aponta que estas três dimensões estão sobrepostas, porque cada uma delas apresenta áreas de interação com as demais, onde eventuais modificações numa das dimensões geram efeitos sobre as demais dimensões. Este pensamento é embasado no sistema social, desencadeando opções e relações empreendidas no ambiente sistêmico.

Junto à visão sistêmica, surge o modelo CESM (*Composition – Environment – Structure – Mechanism*), que permite, dentre outras coisas, perceber com maior clareza os componentes, ligações e processos que envolvem os atores de um sistema.

Segundo Kern (2011) o modelo CESM, é um modelo ontológico, que traz a ideia de sistemismo, consistindo basicamente em que "toda coisa, seja concreta ou abstrata, é um sistema ou um componente ou potencial componente de sistema", ou seja, há uma ubiquidade dos sistemas, uma crença de que não há nada permanentemente isolado e, por isso, é aconselhada a adoção de uma visão sistêmica.

Alguns postulados do modelo de Bunge são: a)colocar todo fato social em seu contexto mais amplo (ou sistema); b) cada sistema em sua composição, ambiente e estrutura; c) distinguir os vários níveis de sistema e exibir suas relações; d) procurar os mecanismos que mantêm um sistema funcionando ou levam à sua decadência ou crescimento; e) verificar se o mecanismo proposto (verificar variáveis e hipóteses) é compatível com leis e normas relevantes e conhecidas; f) preferir hipóteses, teorias e explicações dinâmicas às fenomenológicas, dando preferência às descrições dinâmicas; e g) em caso de mau funcionamento do sistema, examinar todas as fontes tentando reparar o sistema (KERN, 2011).

Considerando, portanto, que tudo é sistema ou faz parte de um sistema, este trabalho utilizará a visão sistêmica como base de pesquisa, partindo do pressuposto de que o processo de difusão e adoção é um sistema social e analisando a tecnologia em estudo como um sistema, a fim de reconhecer suas relações, seus componentes, estrutura e mecanismos, tentando entender as barreiras envolvidas, ou seja, os impactos e alguns possíveis cenários.

Ainda, quanto à caracterização, este trabalho será analisado pela sua natureza, abordagem, objetivos e pelas técnicas utilizadas.

### 3.1.2 Quanto à natureza

Quanto à natureza é considerada uma **pesquisa aplicada**, caracterizada pelo seu principal resultado: uma análise de impacto baseada em modelos conceituais que define os elementos, conceitos e relações e um processo estudado, ou seja, segundo Silva e Menezes (2005), gera conhecimentos para aplicação prática, dirigidos à solução de problemas específicos, envolvendo verdades e interesses locais.

### 3.1.3 Quanto à abordagem

Em se tratando de uma pesquisa aplicada, adota-se uma **abordagem qualitativa**, pois segundo Creswell (2010) é um meio para explorar e para entender o significado que os indivíduos ou grupos atribuem a um problema social ou humano; ela "é uma pesquisa interpretativa, com o investigador tipicamente envolvido em uma experiência sustentada e intensiva com os participantes" (CRESWELL, 2010, p. 211)

Gerhardt e Silveira (2009) colocam que a pesquisa qualitativa se preocupa com o aprofundamento da compreensão de um grupo social ou de uma organização.

Segundo Minayo (2008) a expressão mais comumente usada para representar o tratamento de dados de uma pesquisa qualitativa é a análise de conteúdo, uma vez que diz respeito a técnicas de pesquisa que permitem tornar replicáveis e válidas inferências de dados de um determinado contexto, buscando a interpretação cifrada de material de caráter qualitativo.

Do ponto de vista operacional, a análise de conteúdo parte de uma primeira leitura das falas, depoimentos e documentos e atinge um nível mais profundo, relacionando estruturas semânticas (significantes) com estruturas sociológicas (significados). Esta técnica possui diversas modalidades, dentre elas a análise temática. (MINAYO, 2008).

### 3.1.3 Quanto aos objetivos

Quanto aos objetivos, configura-se como uma **pesquisa exploratória**, pois segundo Gil (2010) estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. A fim de atingir o objetivo desta pesquisa precisamos do aprimoramento de ideias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, envolvem levantamentos bibliográficos; entrevistas, dentre outras técnicas.

Ainda sobre o ponto de vista dos objetivos, é uma **pesquisa descritiva**, que para Gil (2010) visa descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados, neste caso, optou-se por entrevistas abertas.

### 3.1.4 Quanto a coleta de dados

Em relação à coleta dos dados optou-se pela realização de entrevistas semiestruturadas, onde em relação aos aspectos éticos, seguiu a Resolução 466/2012, que regulamenta pesquisas com seres humanos, no qual os participantes do estudo assinaram o Termo de Consentimento Livre e Esclarecido - TCLE (APÊNDICE C), como concordância à participação do mesmo, após orientações sobre a pesquisa.

Para seguir o sigilo, os participantes foram identificados com o código E de entrevistado, seguido do número respectivo à ordem de entrevista, exemplo E1 (Quadro 10).

**Quadro 10 : Lista de entrevistados por órgão/setor**

| Código do Entrevistado | Setor |
|---|---|
| **E01** | Justiça |
| **E02** | |
| **E03** | |
| **E09** | |
| **E14** | |
| **E15** | |
| **E16** | |
| **E20** | |
| **E25** | Membro internacional |
| **E04** | Ministérios |
| **E05** | |
| **E08** | |
| **E06** | Unidades Certificadoras |
| **E07** | Saúde |
| **E10** | Sindicatos ou Associações |
| **E11** | |
| **E12** | |
| **E13** | |
| **E18** | |
| **E17** | Bancário |
| **E19** | ITI e/ou Comitê Gestor ICP-Brasil |
| **E21** | |
| **E22** | |
| **E23** | |
| **E24** | |
| **E26** | |

| | |
|---|---|
| **E27** | |

Fonte: IGTI (2013)

O processo de abordagem para a realização das entrevistas constou do contato prévio por e-mail ou telefone, para agendamento das entrevistas.

As entrevistas semiestruturadas realizadas com os vinte e sete especialistas indicados, foram norteadas por um roteiro de entrevista, composto de 36 questões (APÊNDICE D) distribuídas em dimensões, onde se levou em consideração a colocação de Minayo (2008):

> [...] na verdade nenhuma interação, para finalidade de pesquisa, se coloca de forma totalmente aberta ou totalmente fechada. [...] a semiestruturada obedece a um roteiro que é apropriado fisicamente e utilizado pelo pesquisador. Por ter apoio claro na sequência das questões, a entrevista semiaberta facilita a abordagem e assegura, sobretudo aos investigadores menos experientes, que suas hipóteses ou seus pressupostos serão cobertos na conversa (MINAYO, 2008, p. 267)

As entrevistas foram realizadas por integrantes do IGTI e algumas vezes acompanhadas de membro do ITI, normalmente nos órgãos do entrevistado, no período de Março a Abril do ano de 2013.

Todas as entrevistas foram gravadas em áudio e transcritas na íntegra, o que permitiu o início da análise dos dados.

O tempo de entrevista variou entre 30 minutos a 2 horas.

#### 3.1.4.1 Busca sistemática para mapeamento da Certificação Digital no Brasil

Foi realizada uma busca sistemática da literatura em bases de dados nacionais e internacionais onde foi feito um levantamento de artigos, dissertações e teses referentes à certificação digital no Brasil, a fim de entender como este tema está sendo abordado no Brasil e quais os maiores focos de pesquisa.

A primeira etapa da busca sistemática foi a determinação das bases de dados e da escolha das variáveis para a realização das buscas pelas publicações acadêmicas, onde foram escolhidas as bases Scopus, SciELO e Portal da CAPES.

Com relação ao Banco de Teses e Dissertações (BTD), foram escolhidas a Biblioteca Nacional Brasileira de Teses e Dissertações da IBICT, Sistema Integrado de Bibliotecas da Universidade de São Paulo – SibiNet e o Sistema de Biblioteca da UFSC.

A fim de complementar estas buscas, recorreu-se ao Google Acadêmico na busca de artigos nacionais publicados em eventos ou em revistas não indexadas, e de teses e dissertações que por ventura não tenham sido encontrados nos BTDs mencionados.

A seleção das palavras-chave utilizadas no processo de busca foi determinada mediante a relevância das mesmas ao propósito desta pesquisa.

**Termos de busca da revisão sistemática**[5]

| |
|---|
| Certificação Digital |
| Certificado Digital |
| Infraestrutura de Chaves Públicas |
| ICP-Brasil |
| Assinatura Digital |

Fonte: O autor

O processo de busca nas bases de dados obedeceu aos seguintes critérios e delimitações:

- Para a busca das palavras-chave foram consideradas as palavras exatas;
- Recorreu-se ao operador lógico "OR" para combinação das palavras-chave utilizadas para rastreamento das publicações;
- Limitou-se a busca por publicações no âmbito do Brasil;
- No Portal da CAPES limitou-se a busca por periódicos revisados por pares;
- Na base de dados Scopus limitou-se a busca por artigos que contivessem estritamente em seu título uma das variáveis.

A busca compreendeu o período de 1999 a setembro de 2014 e resultou em 27 artigos e 74 teses/dissertações, que foram analisados e

[5] Na base de dados Scopus a busca foi realizada a partir das palavras-chave em inglês (*digital certification*; *digital certificate*; *Public Key Infrastructure*; *digital signature*)

classificados de acordo com o foco principal, abordado em cada uma delas.

Das 101 publicações selecionadas, dentre artigos, dissertações e teses, percebe-se que o maior número de publicações é de dissertações e teses, totalizando 74 publicações.

Em relação a relevância do assunto, o número de publicações ainda é considerado pequeno para um período de 15 anos.

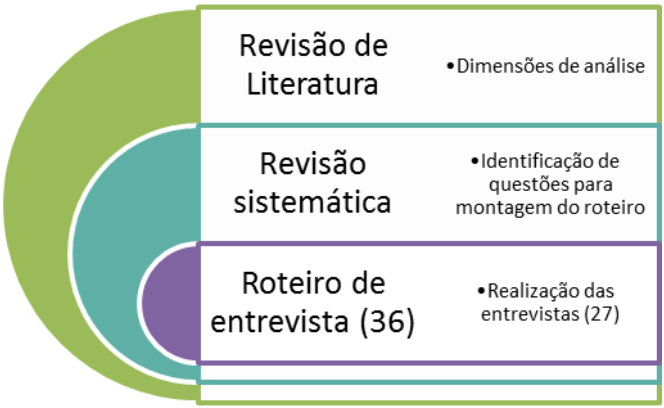
Após as primeiras apreciações resultantes da busca sistemática, foram selecionadas para análise as publicações cujo foco principal era a certificação digital, o que resultou na análise integral de 13 artigos e 30 dissertações e teses, ou seja, 43 publicações.

As publicações analisadas na íntegra foram agrupadas de acordo com o foco da pesquisa, em quatro categorias: (i) **total aderência ao tema certificação digital no que concerne a aspectos teóricos** (totalizando 11 publicações); (ii) **impacto do uso da certificação digital no Brasil**(totalizando 4 publicações); (iii) aplicações da certificação digital (totalizando 23 publicações) e (iv) trabalhos cujo teor fazem uma análise crítica da ICP-Brasil: dos normativos e jurídicos aos aspectos técnicos (totalizando 5 publicações)

### 3.1.4.2 Identificação das temáticas

Com base na composição das oito dimensões encontradas na literatura, sendo: Ambiental, Cultural, Econômica, Legal, Política, Social, Tecnológica e Territorial e considerando os impactos identificados na revisão sistemática, onde a certificação digital (1) promove a segurança aos dados de programas governamentais, da tramitação de processos e demais transações eletrônicas; (2) facilita a arrecadação de impostos;(3) assegura um melhor controle dos programas de governo; (4) dá mais celeridade à tramitação de processos; (5) aumenta a transparência das ações governamentais; (6) promove a desmaterialização dos processos; (7) economia de tempo; (8) bem como autenticidade, confidencialidade e integridade de dados, validade jurídica, entre outras questões; foram formulados questionamentos distribuídos entre as oito dimensões (Figura 18).

**Figura 18: Definição do Roteiro das entrevistas**




Fonte: o autor.

Retomando que as oito dimensões se deram a partir do referencial baseado em Mendes (2009), Angeloni (2002) e Marques (2008) notou-se a necessidade de condensar tais definições, trazendo-as para um foco mais adequado a esta pesquisa, conforme Quadro 11:

**Quadro 11: Definição das dimensões de análise da Certificação Digital ICP-Brasil**

| Dimensão | Definição |
|---|---|
| Ambiental<br>A | Diz respeito aos recursos ambientais, às medidas que resultam na proteção do meio ambiente, como a redução do desmatamento, redução de emissão de poluentes (gases e resíduos), dentre outras questões que auxiliem a reduzir intervenções humanas na natureza. |
| Cultural<br>C | Diz respeito à cultura de cada local, ou seja, sua tradição, seus costumes, suas crenças, seus valores. Está relacionado ao bem-estar, à busca pelo desenvolvimento individual e à formação de uma identidade cultural. |
| Econômica<br>E | Diz respeito às relações de trabalho, lucratividade, investimentos, desenvolvimento econômico, modelo de negócio, modernização dos instrumentos de produção; pesquisação científica e tecnológica, distribuição de renda. Diz respeito ao crescimento econômico e a capacidade produtiva. |
| Legal<br>L | Diz respeito ao cumprimento da Lei e das questões legais que sirvam para estabelecer padrões mínimos de segurança |

| | |
|---|---|
| Política<br>P | Diz respeito à democracia, aos direitos humanos; ao desenvolvimento da capacidade do Estado para implementar projetos nacionais, que visem a coletividade e ao interesse comum. Diz respeito a atitudes de governo em relação a assuntos de interesse público para o bem público. Está relacionado a ações de governo para segurança, economia, cultura, ambiente, tecnologia, inovação, dentre outras questões, dentro e fora de seus limites geográficos. |
| Social<br>S | Diz respeito à igualdade de direitos e condições, bem como igualdade de renda, de qualidade de vida e de acesso aos recursos e serviços sociais. Diz respeito às estruturas, grupos e organizações sociais e suas interações; ao conhecimento e à informação. |
| Tecnológica<br>T | Diz respeito a *hardware* e *softwares* que auxiliam a gestão e disseminação de conhecimentos, bem como a capacitação de seu uso para fins específicos. Está relacionado a produtos e processos. |
| Territorial | Diz respeito às delimitações geográficas e restrições estruturais do país, bem como às relações com outros países. |

Fonte: o autor (2014).

Tendo em mãos o roteiro das entrevistas e os nomes dos 27 entrevistados, partiu-se para realização das mesmas. As entrevistas foram agendadas, por e-mail ou telefone, sendo realizadas por membros do IGTI e algumas vezes com a presença de um representante do ITI, onde além de apresentar a pesquisa, coletar as assinaturas nos TCLE, apresentava-se o roteiro, para que o entrevistado pudesse se guiar.

Desta forma, as entrevistas foram livres para que os entrevistados não fossem influenciados e somente em alguns momentos foi solicitado um maior esclarecimento do contexto em questão.

À medida que iam sendo realizadas as entrevistas, estas iam sendo transcritas na íntegra por membros do IGTI.

Tendo em mãos as 27 entrevistas transcritas (**pré-análise**), foi feita a primeira leitura detalhada destas, a fim de identificar temas (assuntos) recorrentes ou relevantes nas falas dos entrevistados (categorização), onde percebeu-se a necessidade de agrupar estes temas em temas maiores, por semelhança, que chamamos de temáticas (**exploração do material**).

As temáticas identificadas foram distribuídas pelas oito dimensões escolhidas na literatura e codificadas pela inicial da dimensão e pela sequência alfabética, como exemplificado no Quadro 12:

**Quadro12: Definição das temáticas, dimensões e codificação**

| Temas/Assuntos | Temática | Dimensão | Código |
|---|---|---|---|
| Impressão Digital | Biometria | Tecnológica | T-2 |
| Reconhecimento de face | | | |
| Reconhecimento de retina | | | |
| Reconhecimento de voz | | | |

Fonte: o autor.

Foram identificadas 67 temáticas, distribuídas nas dimensões às quais estão relacionadas, ficando distribuídas da seguinte forma: duas na dimensão ambiental; cinco na dimensão cultural; sete na dimensão econômica; 14 na dimensão Legal; 11 na dimensão Política; oito na dimensão Social; 16 na dimensão Tecnológica, e por fim quatro temáticas na dimensão territorial (Apêndice A).

Observa-se que a dimensão com o maior número de temáticas é a dimensão tecnológica, seguida das dimensões legal e política, respectivamente. Já as dimensões com menor número de temáticas são a ambiental e a territorial, seguidas da cultural e da social.

A partir da distribuição das temáticas nas dimensões, procurou-se defini-las, identificando os temas relacionados e explicando o que os entrevistados consideravam em relação a elas, até mesmo para justificá-las dentro das dimensões, o que está detalhado no Apêndice B.

## 3.3ANÁLISE DOS DADOS

Em relação à análise dos dados, optou-se pela utilização da análise de conteúdo, que é uma técnica de pesquisa que visa uma descrição do conteúdo manifesto de comunicação de maneira objetiva, sistemática e quantitativa. (BERELSON, 1984)

Segundo Bardin (2006), a análise de conteúdo consiste em um conjunto de técnicas de análise das comunicações, que utiliza procedimentos sistemáticos e objetivos de descrição de conteúdo das mensagens, tendo como objetivo a inferência de conhecimentos relativos às condições de produção (ou, eventualmente de recepção) das mensagens, podendo-se recorrer a indicadores quantitativos ou não.

Bardin (2006) indica que a utilização da análise de conteúdo prevê três fases fundamentais: 1) pré-análise, 2) exploração do material e 3) tratamento dos resultados –a inferência e a interpretação, que segundo ele:

- Na primeira fase, **pré-análise ou fase de organização**, no caso das entrevistas, é o momento em que elas serão transcritas e a sua reunião constituirá o corpus da pesquisa; devendo-se obedecer às regras de exaustividade (não omitir nada); representatividade (a amostra deve representar o universo); homogeneidade (os dados devem referir-se ao mesmo tema, sendo obtidos por técnicas iguais e colhidos por indivíduos semelhantes); pertinência (os documentos precisam adaptar-se ao conteúdo e objetivo da pesquisa) e exclusividade (um elemento não deve ser classificado em mais de uma categoria).
- A segunda fase consiste na **exploração do material** com a definição de categorias (sistemas de codificação) e a identificação das unidades de registro (unidade de significação a codificar corresponde ao segmento de conteúdo a considerar como unidade base, visando à categorização e à contagem das frequências) e das unidades de contexto nos documentos (unidade de compreensão para codificar a unidade de registro que corresponde ao segmento da mensagem, a fim de compreender a significação exata da unidade de registro). Esta é uma etapa importante, porque vai possibilitar ou não a riqueza das interpretações e inferências.
- A terceira fase diz respeito ao **tratamento dos resultados**, inferência e interpretação. Ocorre nela a condensação e o destaque das informações para análise, culminando nas interpretações inferenciais, onde são destacadas as dimensões da codificação (recorte, agregação ou enumeração, que permite atingir uma representação do conteúdo,

> ou da sua expressão) e categorização (rubricas ou classes, as quais reúnem um grupo de elementos, sob um título genérico) que possibilitam e facilitam as interpretações e as inferências.

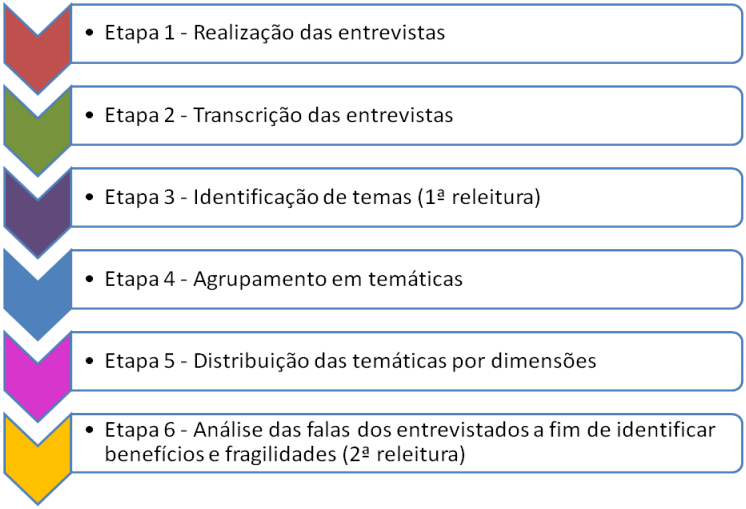
Quando uma pesquisa utilizando análise de conteúdo se dirige à questão "*para dizer o quê*" o estudo se direciona para as características da mensagem propriamente dita, seu valor informacional, as palavras, argumentos e ideias nela expressos, esta pesquisa se constitui em uma análise temática (MORAES, 1999), portanto, após a transcrição das entrevistas, na fase de exploração do material, adotou-se a análise temática.

Os critérios adotados para a categorização dos dados foram os semânticos, que originaram as categorias temáticas, que segundo Moraes (1999) a categorização é o procedimento de agrupar dados considerando a parte comum existente entre eles, onde se classifica por semelhança ou analogia, segundo critérios previamente estabelecidos ou definidos no processo, neste caso, através de critérios léxicos, com ênfase nas palavras e seus sentidos.

Desta forma, a partir da primeira leitura das 27 entrevistas que foram transcritas na íntegra, foram identificados temas recorrentes e relevantes citados pelos entrevistados, que foram agrupados em temáticas (temas gerais), que após foram distribuídas nas dimensões identificadas na literatura.

Distribuídas as temáticas dentro de cada dimensão adotada a partir da revisão de literatura, retomaram-se as entrevistas (segunda leitura), a fim de analisar os comentários dos entrevistados em relação à temáticas, para identificar os benefícios e fragilidades da certificação digital ICP-Brasil. De forma sucinta, a Figura 19 demonstra a sequência das etapas.

**Figura 19: Etapas da análise da pesquisa**




Fonte: o autor.

# 4. ANÁLISE DOS RESULTADOS

Este capítulo tem como objetivo principal apresentar os resultados deste estudo, ou seja, apresentar a análise de impacto da adoção da certificação digital ICP-Brasil na perspectiva de especialistas da área.

## 4.1 PERCEPÇÕES DOS ESPECIALISTAS

A partir do momento em que as dimensões e as temáticas foram definidas, foi criada uma tabela (Tabela 1), onde, a partir da releitura das transcrições das entrevistas foi-se identificando o posicionamento positivo (POS) ou negativo (NEG) do entrevistado, ou quando este somente comentou sobre aquela temática (X), os quais foram designados como benefícios e fragilidades. Cabe ressaltar que as temáticas identificadas refletem no impacto percebido pelos entrevistados/especialistas.

Esta tabulação permitiu identificar a frequência tanto de quais temáticas mais obtiveram posicionamentos positivos, quanto negativos, bem como, quais as dimensões teriam maior impacto na adoção desta ferramenta, a partir da percepção destes especialistas, bem como e as relações existentes entre elas as dimensões.

**Tabela 1: Frequência de posicionamento dos entrevistados em relação às temáticas**

| Dim | Temática | Entrevistado | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| A | A-1 Desmaterialização | POS | POS | POS | POS | POS | POS | POS | X | X | - | X | - | POS | - | - | POS | NEG | - | - | - | - | - | - | - | - | - | NEG |
| | A-2 Economia com transporte | POS | NEG | POS | - | - | - | - | NEG | POS | POS | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| C | C-1 Conscientização do cidadão | - | - | POS | - | - | POS | NEG | - | - | NEG | - | - | - | - | - | NEG | - | NEG | - | X | - | - | - | - | X | - | X |
| | C-2 Conscientização do governo | - | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | X | - | X | - | - | X | - | - |
| | C-3 Conscientização do usuário profissional/ organizacional | POS | NEG | POS | - | - | - | NEG | - | - | - | - | - | - | - | NEG | - | - | NEG | - | NEG | - | NEG | - | - | - | - | - |
| | C-4 Questão cultural | X | - | NEG | - | X | - | X | - | - | - | - | - | NEG | - | - | NEG | - | NEG | - | - | NEG | - | NEG | - | - | - | NEG |
| | C-5 Uso por Terceiros | NEG | X | NEG | - | X | - | - | - | - | NEG | - | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| E | E-1 Agilidade nos processos | - | - | - | POS | POS | POS | - | X | - | POS | - | - | - | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - |
| | E-2 Comércio eletrônico | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | - | - | - | - | - | X | - | - |
| | E-3 Custo do certificado | - | NEG | NEG | NEG | X | - | NEG | NEG | - | POS | - | - | NEG | - | NEG | - | - | NEG | - | - | - | - | NEG | - | X | - | - |
| | E-4 Deslocamento usuário para emissão do CD | X | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | E-5 Economia com estrutura física | - | - | POS | - | - | POS | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | E-6 Melhor aproveitamento de recursos | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS | - | - |
| | E-7 Mercado | - | X | NEG | - | POS | - | POS | NEG | - | X | X | X | - | - | - | - | - | POS | - | - | - | X | - | X | - | - | - |
| L | L-1 Assinatura Digital | - | - | - | - | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | - | X | - | - |
| | L-2 Autenticidade | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | - |
| | L-3 Cadeia de Confiança | - | - | - | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | NEG | X | POS | NEG | - |
| | L-4 Carimbo do tempo | - | - | - | - | - | - | - | - | X | - | - | - | X | - | - | - | - | - | - | - | - | - | - | NEG | - | - | - |
| | L-5 Confidencialidade | - | - | - | - | - | - | X | ´- | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | L-6 Fiscalização | - | - | NEG | - | - | - | - | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | X | NEG | - | - |
| | L-7 Fraudes | - | - | - | - | X | - | X | - | POS | POS | - | - | - | - | POS | - | - | - | - | - | - | - | NEG | - | - | NEG | NEG |
| | L-8 Gestão documental | - | - | - | - | X | NEG | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | L-9 Integridade | - | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | X | - | - |
| | L-10 Lei de acesso | - | - | | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | - | - | - |
| | L-11 Não repúdio | - | - | | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | X | - | |
| | L-12 Segurança tecnológica - jurídica | - | POS | POS | X | POS | POS | POS | X | NEG | POS | X | - | - | POS | POS | - | - | POS | - | - | - | - | - | X | X | - | - |
| | L-13 Sigilo/ Privacidade | - | - | - | - | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | - |
| | L-14 Validade jurídica | - | - | - | - | X | - | X | - | - | - | X | - | - | - | POS | - | - | - | - | - | - | - | - | - | POS | - | POS |
| P | P-1 Conflito de interesse | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | NEG | - | - |
| | P-2 Desburocratização | - | - | - | - | - | POS | - | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | P-3 Governança | - | - | - | NEG | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | P-4 ICP.com X ICP.gov Tipo Estrutura ICP | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | X | X | - | - |
| | P-5 Interorganizações | POS | POS | X | - | POS | - | POS | POS | POS | - | - | - | - | - | NEG | - | - | POS | - | - | - | - | - | - | - | - | - |
| | P-6 Manutenção econômica da estrutura ICP | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | - |
| | P-7 Modelo de negócio adotado | POS | - | NEG | - | POS | X | - | - | - | POS | X | X | - | - | - | - | - | - | X | - | - | - | NEG | X | X | X | NEG |
| | P-8 Modelo de processos | - | - | - | X | POS | - | - | X | X | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | P-9 Novos projetos ITI | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS | - | - | - | - | - | - | - | POS | POS |
| | P-10. Origem da tecnologia com foco na defesa | POS | - | - | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | X | X | X | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | P-11 Rede de Capilaridade | - | - | - | X | X | - | - | - | - | - | - | - | - | - | - | - | - | X | X | - | - | - | - | X | - | - | - |
| S | S-1 Acessibilidade | POS | POS | X | NEG | X | POS | - | X | - | - | - | POS | POS | NEG | POS | - | - | X | - | - | - | - | - | - | POS | - | - |
| | S-2 Cidadania | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | - | - |
| | S-3 Controle Social | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS | - | - | - |
| | S-4 Elitização da CD | X | - | - | X | X | X | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | NEG | - | - | - | NEG |
| | S-5 Inclusão digital | NEG | - | - | X | - | - | X | - | - | - | - | - | - | - | X | - | - | X | - | - | - | - | - | - | X | - | - |
| | S-6 Massificação | - | - | NEG | - | NEG | - | - | X | - | - | NEG | - | - | - | - | - | - | - | X | - | NEG | - | - | NEG | X | - | - |
| | S-7 Transparência | - | - | POS | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | | - | - |
| T | T-1 Atrativos inseridos na tecnologia | - | X | - | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | - | - | - | - | - | - | - |
| | T-2 Biometria | - | - | - | - | X | - | POS | NEG | - | - | - | - | - | - | - | - | POS | - | - | - | - | - | POS | POS | X | POS | X |
| | T-3 Capacitação | X | NEG | X | - | NEG | - | - | NEG | - | X | X | - | - | - | - | - | NEG | X | - | - | - | - | - | NEG | - | - | - |
| | T-4 Criptossistema | - | - | | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | X |
| | T-5 Desdobramentos da tecnologia | - | NEG | - | - | - | - | - | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | T-6 Dificuldade de instalação | NEG | NEG | NEG | NEG | NEG | - | - | - | NEG | - | - | - | - | - | - | - | - | - | NEG | NEG | - | - | - | - | - | - | - |
| | T-7 Ferramenta amigável | - | - | - | - | - | - | X | X | - | - | - | - | POS | NEG | - | NEG | - | - | NEG | - | - | - | | | | | |
| | T-8 Infraestrutura | NEG | X | NEG | NEG | POS | NEG | - | NEG | NEG | - | X | X | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | T-9 Interoperabilidade | POS | NEG | NEG | - | POS | - | NEG | - | - | - | - | - | - | NEG | - | NEG | - | - | NEG | - | - | - | NEG | X | | POS | - |
| | T-10 Logística de emissão/ reemissão do certificado | - | - | NEG | - | NEG | - | - | X | POS | - | NEG | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | NEG | NEG |
| | T-11 Novas aplicações da tecnologia | - | - | X | X | NEG | - | X | X | - | - | - | - | - | - | - | POS | POS | X | - | - | - | - | - | - | NEG | - | - |
| | T-12 Número de aplicações com utilização da tecnologia | - | NEG | - | - | X | - | NEG | - | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | NEG | X | - |
| | T-13 Número de certificados emitidos | - | - | - | - | - | - | - | - | - | - | - | NEG | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS |
| | T-14 Ponto de venda | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | - | - | - | | X | - |
| | T-15 Resistência ao uso | X | - | X | X | - | X | NEG | - | NEG | - | - | - | - | - | - | NEG | - | - | - | - | NEG | - | - | - | - | - | - |
| | T-16 Tecnologia imposta | X | X | X | - | X | X | NEG | - | - | - | X | - | - | - | X | - | - | - | NEG | - | - | X | - | - | | - | POS |
| | T-17 Tempo de emissão/ renovação do certificado | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | NEG | - | - | - | - | - | - | - | - | - | NEG | X | - |
| TR | TR-1 Aquisição de certificados de fora do país | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | NEG | - | | - | - |
| | TR-2 Certificação do passaporte | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS | - | - | - |
| | TR-3 Aceitabilidade em outros países/ Internacionalização | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | X | - | X |
| | TR-4 Migração de certificadoras de outros países | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | POS | X | - | - |

Fonte: o autor

Legenda: POS = Visão positiva NEG = Visão negativa X = Visão Neutra (-) não abordado

A Tabela 1 evidencia os aspectos abordados pelos entrevistados e permite uma visão geral das dimensões analisadas, corroborando ainda para identificar quais as dimensões são abordadas com maior frequência por cada entrevistado e quais as temáticas não foram abordadas pelos mesmos.

De maneira geral, a Tabela 1 permite verificar que as dimensões que mais foram comentadas pelos entrevistados foram: a Dimensão Tecnológica (102 ocorrências), seguida da Dimensão Legal (60 ocorrências; Dimensão Política (51 ocorrências); e Dimensão Social (49 ocorrências), ou seja, a opinião dos especialistas fugiu da perspectiva econômica-tecnológica, convergindo para a perspectiva tecnológica-legal, o que reforça a ideia de que a tecnologia certificação digital está intimamente ligada muito mais às questões legais, do que políticas (pelo grande número de aplicações de governo eletrônico) ou sociais (foco da tecnologia em outros países e que está sendo introduzido aos poucos no Brasil).

Outra observação relevante é que as temáticas apontadas exclusivamente de forma positiva todas as vezes que foram citadas são: Economia com estrutura física; Desburocratização; Novos projetos ITI; Controle Social; Transparência; e Certificação do passaporte.

Já as temáticas citadas exclusivamente sob o aspecto negativo pelos entrevistados que às citaram são: Governança; Manutenção econômica da estrutura ICP; Dificuldade de instalação; e Aquisição de certificados de fora do país.

Na sequência, Tabela 2, são apresentados os principais comentários dos entrevistados para cada temática identificada, bem como o número de ocorrências, o que permitiu identificar quais dimensões e respectivas temáticas são percebidas como de maior impacto, e ainda permitiu identificar os principais benefícios, fragilidades/barreiras, perspectivas futuras e outras unidades de análise.

Dentre as percepções gerais que os entrevistados têm da certificação digital ICP-Brasil, é de que ela é necessária para as organizações e para o cidadão, alguns deles complementam afirmando que essa tecnologia é imprescindível às organizações. O principal fator elencado como benefício da certificação digital é a **segurança**, seja jurídica ou tecnológica, conforme se observa nas falas:

"*Eu não entendo como uma empresa pode trabalhar sem certificação"*[...] *"A certificação é válida e traz segurança, pois login e senha não trazem*" (E02)

"*A ICP-Brasil é o motor da transição de um mundo físico para um mundo digital, onde sua missão é compulsória e inexorável, é o responsável pela transição de um país off-line para um país digital. A necessidade de um instrumento que cumpra esse papel com segurança, não se extingue; a necessidade de identificação de indivíduos, não se extingue, é natural do indivíduo a busca permanente do equilíbrio entre liberdade e segurança*" (E11).

Neste mesmo sentido, o E13 afirma que sem certificação não se pode mais viver, já é um caminho sem volta.

O entrevistadoE14 coloca que há um ganho de segurança, muito mais do que *login* e senha, os dados são sensíveis. É uma garantia a mais, ao analisar o custo x benefício, a certificação digital tem maior impacto em função de segurança. Afirma que o acesso a informação em função da certificação digital, não influenciou outras áreas, são fornecidas informações com certificação digital ou sem certificação digital, o que mudou foi a confiança. No caso de informações judiciais, a certificação digital é sempre uma restrição, um processo em papel e outro eletrônico. São públicos comuns, mas para se ter acesso deve-se fazer parte do mesmo. A certificação digital diminui o espectro por causa da legislação e não favorece uma maior publicidade de informação.

Alguns entrevistados apresentaram *cases* de sucesso que utilizam a certificação digital, como o ComprasNet (Ministério do Planejamento, Orçamento e Gestão – MPOG), o NF-e (da Receita Federal Brasileira – RFB), e o PROUNI (do Ministério da Educação – MEC). Segundo o entrevistado E04, o caso do MEC "representa a agregação necessária a nível de segurança, com uma contrapartida de inclusão e de responsabilização das Universidades".

Diversos entrevistados sugerem que os **processos** devem ser melhorados e, consequentemente, democratizado o uso da certificação digital, pois ainda está bastante elitizado. Assim como salienta-se uma conscientização da população (Pessoa Física), que ainda tem dificuldade de compreender e usar a certificação digital ICP-Brasil. Como se pode perceber através do relato do entrevistado E11:

"*Os processos hoje, são melhores do que eram no passado, mas insuficientes para nossas necessidades do futuro. É como eu vejo a ICP-Brasil. [...] não discuto a tecnologia. A tecnologia é o que sustenta. A certificação digital é a criptografia assimétrica. [...] Estamos tendo tempo suficiente para reanalisarmos o processo. [...] A mera análise do conjunto normativo, nos leva a uma série de fragilidades de processos. [...] Se hoje com o poder de polícia que o ITI tem, ele pedisse para que*

*todas as ACs varressem as suas bases de dados e informassem, ao órgão que os fiscaliza, quantos certificados ativos tem com o mesmo endereço de e-mail, nós ficaríamos aqui pasmos. Processo, governança, riscos sistêmicos... nada disso nós abordamos ainda. O grande risco hoje é o processo*". [...] "*Ninguém vai pôr um convencimento, por uma necessidade, ele vai pôr uma obrigatoriedade. Esse é o modelo hoje: só adquire certificado, aquele que é obrigado*".

Em relação a **normas e legislações**, os entrevistados E03, E04, E05, E07, E08, E11 corroboram que há a necessidade de proposição de normas, leis, diretrizes e padronizações da certificação digital.

Em relação a necessidade de **planejamento e desenvolvimento de estratégias** de implantação e massificação, os entrevistados E01, E03, E04, E05, E06, E07 e E08: mencionam que há a necessidade de planejamento e estratégias na implantação da certificação digital.

Em relação a existência de um **Plano B**, os entrevistados E01 e E05 concordam que não existe um plano B para a certificação digital, que é um caminho sem volta. Neste sentido, o entrevistado E08, sugere que deva ser pensando em um plano B.

Em relação à **massificação da tecnologia**, o entrevistado E03 sugere políticas de regulação para incluir o cidadão, de maneira a fornecer certificado digital gratuitamente, como é feito com a identidade; ou a um preço simbólico.

Ainda neste sentido, o entrevistado E13 coloca que é preciso "*melhorar processos e consequentemente democratizar o uso, porque o uso ainda está muito elitizado*".

Em relação aos benefícios percebidos, foram identificadas, diversas implicações positivas com o uso da certificação digital, além da segurança já mencionada, são destacadas: economia de papel, agilidade nos processos, acesso a informação, entre outros.

Salienta-se que a **validade jurídica** dos documentos digitais, mencionada pelo entrevistado E07 como um ganho significativamente relevante que a certificação digital proporciona.

Em relação à **agilidade nos processos**. De forma resumida, o que antes necessitava de uma série de etapas que dependiam da presença física dos clientes e do dispêndio de funcionários na organização, no modelo atual, com a certificação digital, esses processos são automatizados e validados, possibilitando assim maior agilidade nos processos.

Em relação ao **controle social**, foi relatado que graças a certificação digital, há uma forma de acompanhamento social mais intensa sobre as ações e decisões do governo. Como exemplo em sua instituição: "é uma forma de pressionar os juízes que, sabendo de que há uma forma de acompanhamento social muito intensa em cima [dos processos judiciais], passasse a ter uma postura mais enérgica para que o processo tivesse um andamento mais rápido" (E03).

Sobre **transparência** foi comentado, também pelo entrevistado E03, como um benefício que a certificação digital proporciona ao cidadão. Além disso, ele observa ainda que esse benefício implica diretamente na diminuição da corrupção. Sendo este, um novo ganho proporcionado pela certificação digital.

Já em relação às fragilidades/barreiras percebidas, apontam: É notória uma deficiência na **infraestrutura**, no caso da certificação, a própria lei reconhecendo as dificuldades, define a utilização de *login* e senha ou certificação digital (E03).

Em relação à **massificação da certificação digital** se avançou pouco nessa frente nos últimos anos. "Pensava que fosse ter um crescimento mais consistente, mas isso não se verificou, a certificação digital por pessoa física (cidadão em geral)" (E08).

O entrevistado E16relata que é percebida certa **resistência ao uso** da certificação digital, mas também "um alívio quando na sua utilização, há uma desmaterialização dos processos, sem papel no nosso escritório. Há uma dificuldade na utilização, mas não é a certificação digital, o problema é técnico, a utilização automática às vezes faz parar de funcionar, o sistema é muito volátil. O usuário tem dificuldade. Além disso, precisa estar compatível com os programas dos computadores."

**Tabela 2: Principais comentários dos entrevistados e contagem de ocorrências**

| Dimensão | Temática | Comentários (com base na análise das entrevistas) | Número de ocorrências | | |
|---|---|---|---|---|---|
| | | | NEG | POS | X |
| **Ambiental A** | **A-1 Desmaterialização** | **E01:** Coloca que em relação à percepção da economia de papel, muitas vezes é confundida com o uso da CD e não somente dos sistemas computacionais.<br>**E02: "**se faz análise de custo, para perceber. Já está caminhando a passos largos". "Isso vale a pena".<br>**E04, E05 e E11**: comentam a preocupação com o legado, ou seja, com os documentos em papeis. Como questiona o entrevistado E05: "como promover a desmaterialização disso?".<br>**E13:** coloca dois fatores para a desmaterialização: consumo próprio e substituição do original.<br>**E16:** comenta que a certificação digital proporciona um alívio com relação a desmaterialização dos processos em sua organização.<br>**E27:** "a ideia era construir com o Ministério do Planejamento, um plano para incrementar, considerando que a sociedade andou mais rápido do que o governo, poxa, "vamos fazer a Administração Pública Federal", por que nós temos níveis de gestão, não podemos nos intrometer nas administrações das unidades da federação, que tem autonomia, mas o governo federal tem um poder indutor, vamos trabalhar, vamos impulsionar dentro da Administração Pública Federal, do governo federal, um processo mais arquitetural, mais massivo, mais organizado, [...] um órgão vai e desenvolve um negócio, mas o outro órgão não tem nada, não tem ninguém, não desenvolve nada, "vamos fazer uma arquitetura, vamos construir um plano", começamos com o Ministério do Planejamento, que é quem, especificamente, uma secretaria que tem de certa forma, a área de TI no governo Federal é muito horizontal, não tem ninguém que coordene". | 2 | 9 | 3 |
| | **A-2 Economia com deslocamento/ transporte** | **E03 e E09:** colocam como benefício da certificação digital a redução de custos com manutenção de espaço físico.<br>**E03**: "Não dava para continuar com este custo, alugando prédios caríssimos para se trabalhar com arquivo de processos em papel, com custo para a sociedade imenso, quando nós temos hoje tecnologia de ponta que nos permite fazer este serviço com muito mais eficiência e menos dispêndio de recursos". Afirma ainda que, apesar de a experiência com a certificação digital ser recente, desde 2008, percebeu-se que houve uma diminuição de atendimento presencial na sua organização. Isso se deve ao fato da implementação do peticionamento eletrônico via certificação digital. Ou seja, toda aquela demanda presencial para um advogado dar entrada em uma petição, agora é feita remotamente. | 2 | 5 | - |

| | | | | | |
|---|---|---|---|---|---|
| | | **E09:** Coloca que não há mais a necessidade de deslocamento para abrir ou acompanhar um peticionamento. | | | |
| **Cultural C** | **C-1 Conscientização do cidadão** | **E03:** Coloca que o próprio cidadão que antes não sábia o que estava acontecendo, hoje vai desde júri televisionado, etc.....como uma forma de pressionar os juízes que sabendo de que há uma forma de acompanhamento social muito intensa em cima disso passasse a ter uma situação mais enérgica para que o processo tivesse uma marcha mais rápida.<br>**E07:** Coloca que ainda falta conscientização do cidadão, e do profissional: O que é? Para que serve? Qual a importância? Dentre outras questões.<br>**E10:** Relata que ainda falta conscientização. Que as pessoas não acham mais que os certificados são caros. Coloca que o processo está dando certo, tem que ser mantido.<br>**E16**: Coloca que como Pessoa Física a população não tem a consciência, ainda não sabem o que fazer com a Certificação Digital. Coloca que devem ser ampliadas as informações a respeito da certificação digital: assinatura de e-mails, assinatura profissional, novas aplicabilidades, assinatura de documentos (contratos, planos de saúde). Observa que os benefícios são pouco percebidos, pois há pouca divulgação, os benefícios da certificação digital são mal comunicados. É uma questão cultural.<br>**E18:** Afirma que falta conscientização e informação mesmo para as pessoas. Coloca que é preciso mudar ainda a cultura, pois as pessoas ainda não compreendem o potencial das TI e isso inclui a certificação. Por isso a importância de capacitar, promover eventos explicativos. | 4 | 2 | 3 |
| | **C-2 Conscientização do governo** | **E04:** Coloca que não há uma análise crítica de quais são os serviços que efetivamente empregam, quais são os serviços que um emprego de certificação digital trariam ganhos significativos. Acredita que esses impactos, que os desdobramentos que venham ocorrendo dentro do governo, além dos benefícios que eles trazem em termos desse melhor controle, dessa redução de riscos de segurança para esses sistemas, eles introduzem uma cultura de certificação digital entre gestores públicos, potenciais formuladores de políticas públicas, que também podem ter esse aspecto. | - | 1 | 4 |
| | **C-3 Conscientização do usuário profissional/ organizacional** | **E07:** Coloca que não se pode obrigar os profissionais a substituírem suas carteiras profissionais pelas com certificação e que adquiram sistemas com certificação, até porque o custo é alto.<br>**E15:** Comenta que a iniciativa privada não vai ter interesse, na promoção de políticas agora. Por enquanto as organizações privadas vão continuar usando *login* e senha, que é mais barato. Considera ainda que o poder público é ao contrário, pois existe uma relação de custo benefício, além disso, se o poder público capitanear o uso da certificação digital, | 6 | 2 | - |

| | | | | | |
|---|---|---|---|---|---|
| | | reduzindo custos e consequentemente com a população tendo certificados, então a iniciativa privada vai começar a aderir. | | | |
| | **C-4 Questão cultural** | **E01:** Em relação ao aspecto cultural, comenta que muitas pessoas ainda não se adaptaram a leitura digital e acabam imprimindo os documentos para realizar a leitura.<br>**E07: "**Eu tenho no meu *ipad* muito livros, e gosto de sentir o toque, de tê-lo fisicamente, eu posso até ter no *ipad*, mas o livro tem que estar no papel até para cheirar, tocar, o livro prá mim tem uma visão mágica, é impressionante".<br>**E23:** Explica a diferença da "semente plantada" no Brasil e na Espanha. Coloca que as pessoas têm visto a certificação digital ICP-Brasil como uma forma de monitoramento. Se esta ideia não for mudada, esta tecnologia não será aceita. É necessária uma mudança de cultura. | 7 | - | 3 |
| | **C-5 Uso por Terceiros** | **E01:** Não acredita que existam riscos de implantação ou utilização da certificação digital a não ser que um mau uso resulte numa dificuldade de uso da certificação digital.<br>**E02:** "A OAB está dando treinamento, mas têm idosos. Ele tem que ir para o cursinho da OAB, então leva o neto, que entende de tecnologia, que não sabe nada de jurídico, um com 10 e um de 80. Quem vai advogar? (criou-se o apelido para ele de processo eletrônico, processo vô e eletrônico neto). Por incrível que pareça os próprios juízes pela resolução da justiça do trabalho baixaram da plataforma e criaram uma resolução, onde o juiz terá duas certificações: uma para o assessor fazer o processo todo e outra para o juiz assinar".<br>**E03:** "Quando você empresta o certificado para alguém ele pode fazer coisas por você, e a lei é bem clara, você tem a responsabilidade jurídica e legal, por todos os atos executados por aquele certificado [...] ele está dando a própria assinatura dele, que pode ser usada para o bem e também para o lado mal".<br>**E05:** "Eles sabem o que significa estar emprestando o seu certificado. Se nós pegarmos a norma de segurança, a ISO 27000, que trata de todos os aspectos de segurança da informação, e avaliarmos os pilares dessa norma, isto é, que segurança da informação é tecnologia, processo e pessoas. Então, veremos que não adianta ter um processo forte, uma tecnologia fortíssima, igual a certificação digital, e a pessoa fraca. Eu posso investir em tecnologia e em processo o tanto que for [...] não adianta todo o aparato de segurança, vai do usuário. [...] a partir do momento que eu entrego o meu certificado pra alguém usar, pronto! Eu já burlei toda a infraestrutura de chave-pública brasileira. A partir daquele momento ali, furou. Quer dizer, eu estarei assinando um documento em nome de outra pessoa. E o pior, você não pode dizer que não foi você".<br>**E10:** "Você empresta a sua carteira de motorista para alguém dirigir para você?" | 4 | - | 2 |

| | | | | | |
|---|---|---|---|---|---|
| **Econômica E** | **E-1 Agilidade nos processos** | De forma resumida, os entrevistados colocam que o que antes seria necessário uma série de etapas que dependiam da presença física dos clientes e do dispêndio de funcionários na organização, no modelo atual, com a certificação digital, esses processos são automatizados e validados, possibilitando assim maior agilidade nos processos.<br>**E05:** Coloca que além da questão, da certificação ser, basicamente, agregar segurança ao processo, então, se a gente confia na cadeia de certificados, confia na chave que está aqui dentro, eu confio nessa segurança. Em relação ao processo, se vamos pegar o processo com duas perspectivas, primeiro na perspectiva de agilizar mesmo. Então, um processo igual lá no judiciário, que começa sempre eletrônico, assinado digitalmente, a velocidade de evolução é, abstraindo o tempo que o magistrado leva para ler qualquer que seja o processo, e decidir a respeito. Mas o processo em si, da evolução é muito grande, você vê que não precisa imprimir, não precisa ir no cartório.<br>**E20:** Comenta que a certificação não agiliza a justiça, não melhora o atendimento jurisdicional. | 1 | 4 | 1 |
| | **E-2 Comércio eletrônico** | **E03:** "a aderência das compras eletrônicas via certificado digital, irá proporcionar um crescimento e uso fugaz da tecnologia. Os bancos é uma forma muito grande hoje no mercado de internet. O uso de *login* e senha para o internet *bank* está ficando com seus dias contados a tendência é que os bancos passem a usar a certificação digital. Se o sistema bancário passar a exigir certificação para ingresso ao internet *bank* e *e-commerce* todo passar a utilizar esta tecnologia para fins de acesso a compras na internet, que está crescendo de forma bem visível, eu acho que o futuro da certificação digital é a gente usar igual a um cartão de crédito, cada um tem um, ou você tem ou você não se relaciona". | - | 1 | 2 |
| | **E-3 Custo do certificado** | **E02, E03, E04, E05, E07 e E08**: colocam que os certificados são caros e isto pode dificultar sua massificação.<br>**E03**: Comenta que há uma disparidade muito grande na emissão do certificado, e "isso a gente vê que é um mercado que abusa. Na medida em que isso se tornar uma coisa mais universalizada com maior volume de usuários, eu acredito que a concorrência também vai aumentar por razões obvias. Se tem mais gente comprando, este preço tende a ficar dentro de um patamar mais justo, e caso se transforme em algo extremamente estratégico o governo acaba fazendo uma política de regulação igual faz com a gasolina". Coloca ainda que falta uma padronização e controle do custo do certificado, custo alto e sem qualidade dos serviços de emissão.<br>**E18:** Enfatiza que o custo é a principal barreira. | 9 | 1 | 2 |

| | | | | | |
|---|---|---|---|---|---|
| | **E-4 Deslocamento usuário para emissão do CD** | **E08:** Coloca que quando se fala em pegar um estado que não é um estado muito fora de infraestrutura, por exemplo, Rio Grande do Sul é um estado que tem uma infraestrutura boa, para fazermos um estudo de massificar, para o interior tem muito pouco ARs envolveria deslocamento para atender as unidade ou deslocar alguém para fazer isto e perder um dia inteiro, então não é uma operação muito simples ainda se eu tivesse, por exemplo, em toda cidade com mais de 20 mil habitantes uma AR ou coisa do tipo certamente teria muito mais facilidade de estar operando mais hoje isso está bem longe da realidade. | 1 | - | 1 |
| | **E-5 Economia com estrutura física** | **E03:** Afirma que, apesar de a experiência com a certificação digital ser recente, desde 2008, percebeu-se que houve uma diminuição de atendimento presencial na sua organização. Isso se deve ao fato da implementação do peticionamento eletrônico via certificação digital. Ou seja, toda aquela demanda presencial para um advogado dar entrada em uma petição, agora é feita remotamente. | - | 3 | - |
| | **E-6 Melhor aproveitamento de recursos** | **E25:** Coloca que uma coisa é convencer os cidadãos que é um elemento fundamental que é confiança aos cidadãos e dois convencê-los e as empresas que há eficiência, que vão utilizar seus recursos muito melhor, recursos financeiros, recursos de tempo. | - | 1 | - |
| | **E-7 Mercado** | **E02:** Afirma que é necessária ampliação do mercado; existe certa reserva de mercado das grandes AC's; fomentar alguns nichos de mercado que tem capacidade de ser Autoridade de Registro (AR). Precisa-se de um número maior de empresas operando no mercado.<br>**E03:** "existe certo "monopólio" de mercado; o mercado tem que ser regulado e disciplinado; o mercado abusa dos valores de venda dos certificados digitais".<br>**E05:** Coloca que algumas AC's têm condições de fazer negócio com certificado digital com grande potencial de negócio, tendo o governo como seu principal cliente.<br>**E08:** Comenta que falta trabalhar junto ao mercado para convencionar certas diretrizes; a demanda não cresce, pois fica a aguardando o mercado evoluir e o mercado fica aguardando a demanda evoluir (círculo vicioso).<br>**E11:** Coloca que ainda há uma visão distorcida com relação aos movimentos de mercado. Não acredita que será o foco, tão cedo, das políticas públicas. Afirma ainda que essa "demora" do mercado não é uma espera, mas um vetor, uma massa crítica, onde o governo tem papel indutor. No momento em que qualquer tecnologia tem dimensão de impactar negócios, então o negócio irá evoluir, pois os empresários farejam resultados. | 2 | 3 | 6 |
| **Legal L** | **L-1 Assinatura Digital** | **E22:** Coloca que grandes bancos com grande infraestrutura tiveram dificuldade de implementar assinatura, imaginem os outros.<br>**E25:** Coloca que a Assinatura digital, por lei é a que tem a máxima garantia jurídica, e isto | - | - | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | é fundamental. | | | |
| | **L-2 Autenticidade** | **E25:** Coloca que há uma escala, há um correio eletrônico que deixa rastro, é um problema de repúdio e ao final está a firma eletrônica certificada, que te garante o repúdio, autenticidade, integridade, validade jurídica, mas isto é um processo. | - | - | 1 |
| | **L-3 Cadeia de Confiança** | **E23:** Coloca que a cadeia de confiança ainda apresenta fragilidades.<br>**E26: "**O que tem de PKI, o que eles chamam de âncora de confiança, que é a AC Raiz, ou seja, o certificado dela é auto-assinado, ninguém diz pra ela quem é ela, ela é ela. Ai você tem alguns pressupostos dessa confiança. Como você estabelece confiança no meio eletrônico, uma maneira de fazer isso, é por meio dos browsers. O browser estabelece essa âncora de confiança, por isso, é que pra você colocar uma raiz num browser é uma complicação, ou seja, a Microsoft fala, eu ponho, mas EU ponho e põe pra todo mundo, mas você tem que me provar quem é você, você é ITI, você é Brasil, me dá ai o seu certificado, e coloco no meu browser e a partir dai eu faço a minha âncora de confiança. Os outros navegadores a mesma coisa, temos um problema com o Mozzila Firefox. Eu tenho que colocar que eu confio, o problema passa a ser um problema seu. Eu defino a minha âncora de confiança, por ex. eu desenvolvo uma aplicação interna aqui do ITI, falo assim, só aceito CD-ICP-Brasil, então eu defino/estabeleço minha ancora de confiança, ponho na minha aplicação, instalo na minha aplicação o meu certificado raiz (V1, V2, V3). Isso é do ponto de vista técnico tá. Isso é do ponto de vista técnico de âncora de confiança de PKI". | 2 | 1 | 3 |
| | **L-4 Carimbo do tempo** | **E09:** Comenta que a sua organização viabilizou uma estrutura, que quase nenhum órgão tem no Brasil, para garantir o carimbo do tempo, ou seja, a hora legal dos documentos. Coloca ainda que é necessário resolver o problema de aderência do carimbo de tempo: "a gente está carimbando o tempo com as nossas carimbadoras aqui, que o ITI nem sabe que elas existem, então é uma coisa que a gente precisa corrigir".<br>**E24**: Coloca que o carimbo do tempo é uma demanda reprimida na ICP. | 1 | - | 2 |
| | **L-5 Confidencialidade** | **E07:**"Começavam a se expandir software de registros eletrônicos em saúde, em consultórios, clínicas e hospitais, e que tinham pouca ou nenhuma segurança, o acesso era feito através de senha que ficava geralmente com a secretaria, ou na gaveta colado que as pessoas acessavam e a falta crença de que isso autorizava a questão do *paperless*, não precisaria mais papel, e nós ficamos muito preocupados com duas coisas, primeira pela insegurança, que o próprio médico ficava do ponto de vista jurídico porque não tinha validade aquele documento e segundo pela segurança daquele documento, o que nos motivou mesmo foi a segurança, que ai foram vários estudos, vários fóruns de | - | - | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | | confidencialidade, privacidade o ITI também participou, com muito convidados, representantes de software da área médica, o que nós a almejávamos, muito mais do que o prontuário da área médica era a segurança, porque nós temos a questão do sigilo, como uma peça basilar do exercício, pessoas só contam os seus segredos para nós e precisam contar, quase todos ou todos, porque sabem que isso poderá modificar o nosso entendimento sobre a doença, evolução, tratamento necessário, senão houver essa cooperação, geralmente são dados referente a sua intimidade que precisam ser protegidos de qualquer pessoa que esteja fora da relação médico- paciente". | | | |
| | **L-6 Fiscalização** | **E09:** Comenta que necessita de auditoria interna no processo de implantação da certificação digital para garantir que as organizações estejam utilizando a certificação digital da maneira correta. Coloca que hoje se usa CD, mas que nunca passaram por um processo de auditoria interno, para ver se está acontecendo como deveria. | 3 | - | 2 |
| | **L-7 Fraudes** | **E10:** Coloca que há uma redução de fraudes, redução de custos com mala direta, desburocratização, segurança nas transações com validade jurídica.<br>**E23:** Coloca que fraudes vão ocorrer, porque se está comprando governabilidade. O critério técnico é muitas vezes abandonado em prol do critério político. | 3 | 3 | 2 |
| | **L-8 Gestão documental** | **E05: "**Se definiu todo um processo eletrônico, assinado digitalmente, mas a partir de que momento, não se emite mais papel? Como é que eu vou fazer com o legado? Vamos continuar com estes estoques fantásticos de papel que temos pelo país a fora? Qual a validade jurídica de que pegar estes processos? Certificar e guardar eletronicamente? Como isso será feito? Como será o armazenamento? Como será feito seu resgate? Ainda existem algumas perguntas que só serão possíveis responder à medida que for andando com o projeto"**.**<br>**E06:** Comenta que a certificação digital fez repensar os processos. Processos físicos para processos eletrônicos, ou o que se aproximam disto. Antes todos os documentos físicos, agora precisa-se providenciar os trâmites necessários, existem barreiras, precisamos evoluir, os processos eletronicamente estão sendo testados, o sistema está homologado, mas não está funcionando. "Aquele processo que é necessário a assinatura digital as pessoas estão conscientes/esclarecidas sobre o uso da certificação digital. Em relação à segurança neste aspecto. Eu ainda não entendi os processos em termos de relação de guarda, em ciclo de vida destes documentos, até porque o meu processo é de encaminhar, e não de guarda, no caso o ponto final, do receptor. O que eu observei de interessante foi a diminuição na quantidade de papéis, e o trato e o tempo".<br>**E08:**Em relação a gestão documental, exemplifica que "de ferramenta de gestão | 1 | - | 2 |

| | | | | | |
|---|---|---|---|---|---|
| | | documental a ideia é que a gente comece com a autenticação de documentos usuário e senha ele gera um *hash* interno, ai guarda isso num banco e o banco quando alguém for consultar eu uso o A1 para poder validar aquele documento que aquele pequeno banco de dados é uma evolução em relação a consulta usuário e senha sem dúvida mas que pode evoluir ainda mais quando se colocar o certificado já na entrada para ele já vir com a assinatura completa". Afirma que a perspectiva é que se vá incrementando. | | | |
| | **L-9 Integridade** | **E24:** "o poder executivo providenciará pra que sejam reguladas por legislação específica as seguintes matérias, vários itens, e hoje a maioria está dentro de decreto 3.505, de segurança da informação, e lá estava assim "aplicações da criptografia para autenticação do usuário e verificação da integridade de documentos eletrônicos"". | - | - | 2 |
| | **L-10 Lei de acesso** | **E23: "**Se um servidor morre, eu posso abrir sua chave, mas se eu digo para o seu advogado, para um juiz que eu quebro isso, acaba com a cadeia de confiança, então precisa de uma classe especial para fazer isto. Isto é um dilema, e a ICP sabe de sua fragilidade ao negociar comigo este tipo de coisa. É extremamente delicado, porque precisa abrir isso, e é um problema criado pelo próprio governo, aprovando a Lei de Acesso". | 1 | - | 1 |
| | **L-11 Não repúdio** | **E05:** "certificado não permite o repúdio, não é. Então, essa questão inclusive para o nosso usuário, ela é preocupante, o advogado, mais bem preparado em relação ao que representa o não repúdio, é mais fácil de usar, é mais fácil conscientizá-lo de não emprestar o seu certificado com o seu PIN, para fazer qualquer tipo de procedimento ou de acesso, utilizando certificado. Mas e o usuário com um?" | - | - | 3 |
| | **L-12 Segurança tecnológica - jurídica** | **E05**: Coloca que a maior preocupação é com a segurança, em princípio, mas algumas áreas não estão preocupadas com o aspecto econômico.<br>**E09:** Coloca que pode ser que antes, quando era em papel, havia problemas que ninguém percebia e, com a certificação digital, esse maior cuidado já é inerente a tecnologia. Mas tem um problema: falta um amadurecimento. "Falta um tratamento da informação, uma classificação, uma verificação no nível de segurança da informação".<br>**E24:** Afirma que o ponto mais crítico é a identificação presencial, o agente de registro é a parte mais importante na questão de segurança da cadeia. Coloca ainda que a certificação está num conjunto de coisas, ela não vai resolver tudo. Ela é uma das engrenagens da segurança, ela não é a segurança. | 1 | 9 | 5 |
| | **L-13 Sigilo** | **E07:** "Os planos de saúde eles modificaram a técnica, agora você só vai pagar o seu procedimento se você autorizar expressamente, e o médico fica em uma situação muito | 1 | 1 | - |

| | | | | | |
|---|---|---|---|---|---|
| | | difícil, o paciente chegava e dizia, eu quero que você coloque porque se você não colocar vai gerar problemas pra mim neste plano de saúde, e nós não concordamos com isso, pq isso não é um consentimento livre ele é uma coação, então nós ainda estamos agora numa luta com isto, porque o Ministério Público quer abrir quer abrir este sigilo dos pacientes, e como eu disse é um ponto, é uma das bases da medicina, a proteção do sigilo, o sigilo não nos pertence, pertence ao paciente, se ele quiser revelar para os outros problema dele, mas eu sou um depositário fiel guardador, e esse prontuário seja na versão de papel seja eletrônico ele tem que ter uma forma de proteção destes dados e a garantia da não inviolabilidade, esse é o tamanho da motivação que nos fez caminhar, falta muito ainda".<br>**E25:** Comenta que a confiança é uma estrutura horizontal, e isto no Brasil, é uma estrutura vertical, cada um tem seus interesses. | | | |
| | **L-14 Validade jurídica** | **E07:** Coloca que a validade jurídica dos documentos digitais é um ganho significativamente relevante que a certificação digital proporciona.<br>**E11:** "o gatilho deste processo é a validade jurídica do ato da declaração de vontade entre as partes com validade com algum grau de valor probante".<br>**E27:** "o certificado digital ICP-Brasil, ele tem plena validade jurídica, então eu não posso entregar um certificado digital para outra pessoa". | - | 3 | 3 |
| **Política P** | **P-1 Conflito de interesses** | **E23:** Coloca que há um emperramento na disseminação da tecnologia, porque os interesses de governo estão se misturando aos interesses de mercado. | 2 | - | - |
| | **P-2 Desburocratização** | **E10:** Afirma que há uma redução de fraudes, redução de custos com mala direta, desburocratização, segurança nas transações com validade jurídica. | - | 2 | - |
| | **P-3 Governança** | **E11:** Coloca que hoje estamos muito preocupados com a validade jurídica, enquanto em relação a segurança de processos não se evoluiu. "Processo, governança, riscos sistêmicos... nada disso foi abordado ainda. Ainda não existe um modelo de governança. Não tem uma matriz para modelagem de dados que permita um modelo de governança. Infraestrutura de chaves primárias (risco sistêmico)". | 2 | - | - |
| | **P-4 ICP.com X ICP.gov** | **E23:** Coloca que está-se precisando criar o ITI.gov, voltar às origens, pois quando a estrutura inicial foi montada ela não tinha o negócio como foco, era apenas para atender uma necessidade do governo, faltou planejamento, e a tecnologia está sempre se adaptando, criando um segundo chip e logo um terceiro. Coloca que teria que ter uma ICP.com e outra ICP.gov, ambas apenas sob a gestão do governo.<br>**E23:** Coloca que quando a estrutura foi montada ela não era um negócio. Era para atender o | 1 | - | 2 |

| | | | | | |
|---|---|---|---|---|---|
| | | governo.<br>**E24:** "O início da ICP-Brasil é muito centrada em políticas públicas. O grande incentivador é a secretaria da RFB, na obrigatoriedade dos impostos, das transações"…<br>**E25:** "No Brasil a infraestrutura nasceu de uma estrutura de raiz única, que é o modelo Alemão. Na Espanha é uma estrutura completamente de governo. Privada é a contratada. Tudo é estatal. Mas tens que ir com uma fotografia e nada mais. A Identidade custa 12 euros, feita a cada 10 anos. Leva 2 minutos, 5 minutos no máximo". | | | |
| | **P-5 Interorganizações** | **E01, E02, E05 e E06:** Afirmam que há um relacionamento positivo com outras instituições parceiras.<br>**E01:** Menciona que a sua organização promove parcerias que auxiliam na disseminação da certificação digital.<br>**E03:** Comenta em relação ao relacionamento com o ITI, que se deve estreitar um relacionamento com o ITI no desenvolvimento destas tecnologias, para que não se desenvolva a certificação digital sem ter uma visão nacional e macro dos problemas que podem acontecer.<br>**E05:** Informa que tem parceria com a SERPRO. Coloca que são feitas a fim de adquirir certificados através de compras conjuntas e para auxiliar na logística de emissão.<br>**E07:** Informa que tem parceria com a ANVISA, Ministério da Saúde, Sociedade Brasileiro de Informática em Saúde e Conselho de Odontologia. Mas comenta que não há um relacionamento alinhado com outras instituições parceiras. Tem encontrado dificuldade nessa comunicação interorganizacional.<br>**E08:** Informa que tem parcerias com o Conselho Federal de Medicina, FUNAI e Cartório de Engenharia Civil.<br>**E09:** Informa que tem parcerias com TRF – Tribunal regional federal, CJF – Conselho da justiça federal, CNJ – Conselho nacional de justiça, AGU – Advocacia Geral da União, PGR – Procuradoria Geral da República e AC-Jus. Comenta ainda que hoje a sua organização já tem uns 5 órgãos, efetivamente, se relacionando, isto é, trocando informações. Ressalta ainda que é uma meta da administração de sua organização, aumentar o relacionamento com outros órgãos por meio do processo eletrônico.<br>**E15:** "Uma certificadora X chega para o Tribunal e diz: "olha eu vou te emprestar, vais ficar com o prédio X, sem precisar pagar aluguel, já que tu vai utilizar os nossos serviços, tu ficas com o prédio X, sem precisar pagar aluguel, eu também te dou a certificação digital de todo mundo que precisar no teu tribunal, de graça. Só que ai ela não funciona bem, para emitir a certificação digital, ela demora 2, 3, 4 meses pra sair uma certificação, de um usuário". | 1 | 7 | - |

| | | | | | |
|---|---|---|---|---|---|
| | **P-6 Manutenção econômica da estrutura ICP** | **E25:**"o recurso não mantém a estrutura atual, o governo paga para manter a estrutura, o lucro não é repassado". | 1 | - | - |
| | **P-7 Modelo de negócio adotado** | **E05:** "o modelo de negócio para emissão de certificados da Caixa Econômica Federal (CEF) estimula o uso, quer dizer, a caixa tem condições de fazer negócio com Certificado Digital, com os clientes de determinado nível, e dentro dessa ideia de cliente aparece o governo como cliente da CEF. Coloca ainda que para alguns sistemas o certificado é utilizado apenas para segurança, já em outros é para agilizar e segurar os processos, o que impacta nos modelos de negócios".<br>**E06:** Comenta que está na torcida para alguém pensar em um novo modelo de negócio decorrente da certificação digital.<br>**E11:** Não enxerga que os negócios esperam pela certificação digital. "A sociedade não fica refém da tecnologia, de um processo, de uma tendência, de um governo, então no momento que uma tecnologia se mostra útil, ela é incorporada. É necessário aproveitar para aprimorar o modelo vigente da organização, para poder enfrentar um debate público com a sociedade sobre a segurança, de fato, dessa infraestrutura, pois hoje se está muito preocupado com a validade jurídica, mas na segurança de processos não se evoluiu. Processos, governança, riscos sistêmicos, nada disso foi abordado ainda pela organização. Em alguns casos houve um retrocesso". Ele argumenta também, que antes haviam arquivos com documentos, agora, existem cofres cheios de cartões de certificados.<br>**E23:** Coloca que é preciso mudar o modelo de certificação adotado.<br>**E27:** Coloca que a certificação é uma ferramenta hegemonicamente corporativa, dominantemente corporativa. "Como mudar isso? Mudando o eixo, não mudando, mas diversificando esse eixo, além de você ter um eixo de aplicações corporativo/empresarial, você ter aplicações pro uso do cidadão. Enquanto essa passagem não acontecer, é complicado". | 3 | 3 | 7 |
| | **P-8 Modelo de processos** | **E04:** "na nossa organização o modelo de processo consiste em uma transição, em que existem duas formas de acesso: com certificado digital e sem certificado digital".<br>**E05:** Expõe que existe um caso de extremo sucesso, um processo totalmente eletrônico, assinado digitalmente, chegar ao STE. "Isso graças a esse novo modelo de processo com a certificação digital. Na CEF já se faz *login* na rede com certificação digital. Tem a opção com senha também, mas como a maioria dos gerentes já tem certificação digital, então faz *login* com certificado digital".<br>**E08:** "no INSS se tem dois grandes usos da certificação digital, um é para autenticação, para acesso a informação, e num segundo momento, para acesso a realizar transações. Para esse segundo a gente já tem algumas ferramentas em uso, maduro, mas com um público de | 1 | 1 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | usuário relativamente pequeno. Gradualmente ir migrando do *login* e senha para a certificação digital".<br>**E09:** Não atribui a mudança que aconteceu nos processos à certificação digital em si, mas acredita que ela motivou as mudanças que já eram necessárias nos processos eletrônicos.<br>**E11:** Relata que um dos fundamentos de uma PKI (*Public Key Infrastructure*), de uma ICP, é a proteção da chave privativa. O não comprometimento da chave privativa do titular ou da AC é a regra de ouro [...] o processo é o elo fraco, a criptografia assimétrica não. Argumenta que o certificado portátil, permite um comprometimento desta chave privativa. A tecnologia é o que sustenta o processo, e o certificado digital é a criptografia assimétrica. Alega que há tempo suficiente de reanalisar os processos, A mera análise do conjunto normativo nos leva a uma série de fragilidade do processo. | | | |
| | **P-9 Novos projetos ITI** | **E26:** Coloca que tem outras iniciativas, que o ITI está fazendo, que é a AR biométrica, as PPP's com os Estados, mas isto é projeto para 10 anos.<br>**E27:** "Atualmente estamos tendo os chamados *killers-applications*. Estamos tendo anualmente pelo menos uma aplicação nesse tipo. O SPB historicamente foi o grande primeiro sistema usado pelo ICP-Brasil. Então ele tem um papel histórico. Só que ele é muito de bastidor. O cidadão não o percebe tanto. Mas nos últimos 4 anos, temos tido grandes aplicação anuais, conectividade social foi uma delas, o HomologaNet. De certa forma, temos um carro chefe anual". Coloca ainda que o esforço hoje, o maior esforço que o ITI tem hoje, é o tema biometria, do uso da biometria, da inserção, da incorporação, da importação do tema da biometria para dentro da ICP-Brasil, visando a agilidade, a segurança do processo de emissão de certificados. [...] "então a gente precisa fazer um processo mais ágil", [...] "nós vamos inserir muito o tema da biometria, nós temos que inserir a biometria dentro da ICP-Brasil para que aja perspectiva de novas aplicações, para que aja expansão/difusão, sem isso não dá para pensar em um universo desses".[...] "Eu diria que do ponto de vista da plataforma tecnológica, que esse sistema, ele tem várias dimensões, dimensão da tecnologia, algoritmo que usamos, do HSM, da sala cofre, toda essa padronização tecnológica, [...] isso já está certificado. [...] o que nós estamos vendo na prática, nós já sabíamos, todo o sistema tecnológico, sofisticado, por melhor que seja, [...] ele naufraga sempre no fator humano. [...] onde nós podemos melhorar isso, sem transformar a vida do cidadão num inferno, é usando a tecnologia biométrica, eu não vejo outro caminho, pode ser que daqui 1 ano - 1 ano e meio a gente faça uma revisão, isso não é nenhuma verdade sacrosanta, pode ser que na prática...não se viu isso ainda na prática, o piloto que nós tínhamos no DF, com a experiência que nós tivemos nesse 1 ano e meio, a gente diria que esse é o melhor caminho e é onde nós vamos investir, visando a expansão e a difusão dessa tecnologia. Hoje é muito difícil impor ao cidadão comum essa tecnologia". | - | 3 | - |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | **P-10 Origem da tecnologia com foco na defesa** | **E23:** Comenta que todos os países começaram como no Brasil, todos ligados a questão de defesa. "E o que acontece hoje nestes países? (Portugal, Espanha…) Existem duas visões, uma é a certificação do Estado e a outra, da sociedade. Coisas diferentes. Isso funciona em toda a Europa assim. E essa coisa no Brasil, não foi assim. Tudo aquilo que é de inteligência, é quem põe a mão. Mudou muito a visão do que era certificado digital. [...] Quem teria de estar mais preocupado com a segurança, o governo, não atua tanto quanto as empresas privadas".<br>**E24:** "para fazer a ICP-gov, nós estudamos 6 países, estudamos como era na Austrália, na Alemanha, no Canadá, na Inglaterra, na Itália e nos EUA. Dos modelos que a gente estudou, o modelo do Canadá era o mais completo e se constrói toda a ICP-gov em cima do modelo canadense, que não deu certo. Nesta mudança adota-se o modelo nacional da união europeia, através da diretiva 199-93". Coloca que impacto sócio-econômico da certificação digital, que talvez possa ser percebido, na área da educação (todo PROUNI usando certificação digital), na área de medicina (prontuário eletrônico), na área da saúde principalmente, aparecendo muitas aplicações, na área de controle ambiental (licenças ambientais), o cidadão começa a perceber que a certificação tem utilidade, se ele achar que é só para controlar, então ele não vai usar, porque ele já está cansado disso. | - | 1 | 5 |
| | **P-11 Rede de Capilaridade** | **E24: "**Dos quase 20.000 agentes de registros hoje nessa estrutura, dentre ACs e ARs, quase 10mil são dentro da CEF, pela capilaridade de suas agências. As instalações técnicas dos Correios, tem uma capilaridade muito maior do que a CEF. Ponto mais crítico é a identificação presencial, o agente de registro é a parte mais importante na questão de segurança da cadeia". | - | - | 5 |
| **Social S** | **S-1 Acessibilidade** | **E01, E02, E03, E04, E05, E06 e E15**: corroboram que a certificação digital possibilita mais acesso a informação.<br>**E03:** Faz uma importante observação, de que a informação deve estar disponível de forma inteligente para o usuário final. Coloca que é necessário não só disponibilizar informação, mas fazê-la acessível: "a informação deveria vir de forma inteligente para o usuário final, e que seja útil, se não ele lê e busca que possa explicar, aí realmente nós temos horas e horas sendo pagas para atendimento de balcão, quando talvez com algumas ações se pudesse resolver".<br>**E05**: Comenta que há uma facilidade muito maior em buscar a informação, por meio digital, pois o mecanismo de busca é automatizado.<br>**E12:** Coloca que no caso deles, o uso da certificação digital foi um grande negócio, | 2 | 7 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | provocou mais autoestima e será fantástico quando alcançar todas as corretoras.<br>**E14: "**Acesso a informação em função da certificação digital, outras áreas não aconteceu influência, fornece informação com certificação digital ou sem certificação digital, o que mudou foi a confiança. A certificação digital diminui o espectro por causa da legislação. A certificação digital não favorece uma maior publicidade de informação".<br>**E15:** Destaca que a ideia anterior era que o certificado digital restringiria o acesso, o que foi percebido de forma contrária, pois o acesso aos processos aumentou. Em alguns lugares o acesso quadriplicou em relação às consultas de processos em papel. | | | |
| | **S-2 Cidadania** | **E24:** "O conceito de cidadania se percebe dois pontos os serviços públicos e os serviços ao público. Os SI de governo seriam sistemas de gestão de governo. Os serviços ao público, seriam informações de Estado, do sistema de gestão do Estado. Dividia em 4 partes: infraestrutura, desenvolvimento social, econômico produtivo e estratégia e defesa. Para cada um, existem sistemas horizontais do governo, que onde existe uma instalação de governo, eles estão presentes, para dar suporte as funções de Estado.[...]duas características: informações de governo e informações de Estado [...] traz um novo perfil de informática pública.[...] o perfil do desenvolvimento de sistemas mudou um pouco. [...] os sistemas controlavam a cidadania [...] hoje a gente vê [...] a explosão de desenvolvimento de sistemas de atendimento ao cidadão, de prestar serviços ao cidadão". | - | - | 2 |
| | **S-3 Controle Social** | **E03:** Afirma que graças a certificação digital, há uma forma de acompanhamento social mais intensa sobre as ações e decisões do governo. Como exemplo em sua instituição: "é uma forma de pressionar os juízes que, sabendo de que há uma forma de acompanhamento social muito intensa em cima [dos processos judiciais], passasse a ter uma postura mais enérgica para que o processo tivesse um andamento mais rápido".<br>**E24:** "A ICP-edu vai ser importante por 2 aspectos: 1º - que o meio acadêmico e as universidades, vão estar praticando uma tecnologia moderna de alta rotabilidade e sem restrição legislativa, vai poder ser o centro de pesquisa [...] que a gente não pode fazer. (vem para a ICP como um suporte de desenvolvimento) 2º - e ele pode ser posteriormente um agente propagador disso". "O Sucesso no SPED, que está incluindo o e-Social (todas as relações trabalhistas, previdenciárias), que vai ter 3 grandes aspectos: a parte de recursos humanos, a fiscal e a contábil. O e-Social saiu com uma definição de usuário e senha e tem decisões antagônicas dentro mesmo de políticas públicas". Cita a PEC 6/2011, inclusão social como direito social. | - | 2 | - |
| | **S-4 Elitização da CD** | **E01, E04 e E06:** ressaltam o cuidado que se deve tomar para que o processo de implantação da certificação digital não gere uma exclusão social. | 3 | - | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | **E23:** "Acertificação digital está elitizada, porque se tentou massificar a certificação digital através do Banco do Brasil e da CEF, que tem interesses de banco e não de governo. Então o modelo de negócio seguido pela ICP foi viabilizar a ICP como ".com", penetrar bastante no seguimento empresarial para dar segurança a transações eletrônicas. Em nenhum momento se pensou na população em si". | | | |
| | **S-5 Inclusão digital** | **E01 e E15:** Comentam que é um fator de extrema importância que precisa evoluir no Brasil. É necessário promover maior inclusão digital.<br>**E04: "**Esses 11 anos pra mim, eles estão associados a um movimento de inclusão, porque eu só consigo pensar os impactos ideais, se eles são, pelo menos, não restritivo a inclusão de todos, em todas as possibilidades. Então, se eu tiver um programa social que pede certificado digital, ou se eu tenho um brasileiro que pode se candidatar a este e que não tem um certificado digital, então o certificado está aumentando este fosso. E o fosso social, ele tem esse contexto. Acesso à documentação civil básica no Brasil, ainda é um luxo, para pelo menos 10% da população". Coloca ainda, que o pregão eletrônico, com a incorporação de alguns graus do uso de certificado digital, em algumas funcionalidades, ele não é uma iniciativa excludente. "Ele permitiu que o princípio de inclusão de pequena e micro empresa, fosse mantido. [...] porque a gente enxerga nas estatísticas de compras, essa evolução das compras governamentais de pequena e microempresa".<br>**E07:** Comenta que é fato que nas capitais e ou grandes cidades do Sul e Sudeste a inclusão digital é maior, mas qual será a logística de apoio e capacitação nas cidades do interior dos estados, principalmente para outras regiões do Brasil? | 1 | - | 5 |
| | **S-6 Massificação** | **E05:** Em relação à massificação do uso da certificação digital para o cidadão, comenta que é necessário massificar o uso da certificação digital para o cidadão comum, em que ele possa assinar documentos digitalmente, de forma que o documento primitivo, original, seja digital. "O que ocorre ainda é um volume de documentos originais em papel, pois a massificação da certificação digital para o cidadão ainda é pequeno. Hoje, o modelo de assinatura física é o predominante". E alguns entrevistados concordam que essa massificação a curto e médio prazo não é otimista. Afirma que a tecnologia existe, que o processo é fantástico, e que a infraestrutura se mostra cada vez mais estruturada, mas há uma preocupação de como atingir/ viabilizar aos cidadãos de regiões inóspitas/remotas, massificando o uso.<br>**E08:** Coloca que a proposta é ir gradualmente disponibilizando serviço e à medida que disponibiliza serviço, vai dando certificado como um caminho de uso e evolução.<br>**E11:** Acredita que as medidas de governo funcionam como o uso do cinto de segurança, por exemplo. No entanto, verifica a falta de campanhas de massificação da | 5 | - | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | desmaterialização dose processos, em que acredita que só o governo tem condições de fazer. Atualmente, se o ITI, com o poder que possui, solicitar para que todas as AC's façam uma varredura às suas bases de dados, informando ao órgão que os fiscaliza, quantos certificados ativos tem com o mesmo endereço de e-mail, então encontraria um número muito surpreendente.<br>**E24**: Coloca que a massificação do uso da CD é um problema, como resolver isso? | | | |
| | **S-7 Transparência** | **E03:** Relata que outro aspecto da certificação é a diminuição da corrupção, porque quanto mais foco e transparência, é mais difícil os casos de corrupção, que existem e não podemos fugir a realidade. Coloca que essa facilidade no caso da informação diminui o número de atendimentos, facilita para o cidadão comum, ele pode acessar os dados sem precisar ir lá, facilita porque o Judiciário tem mais transparência ao que faz e como faz. | - | 1 | - |
| **Tecnológica T** | **T-1 Atrativos inseridos na tecnologia** | **E02: "**O papel pode ser transitório, com *login* e senha, depois você retira o papel e deixa o *login*, a senha e a certificação digital. A migração vai ser natural, sem excluir um direito fundamental. Trazer atrativos que a pessoa tire o certificado e tire proveito disso".<br>**E05:** "qual for o atrativo que eu acredito que o, que o ITI utilizou para o CRM vir procurar o ITI pra normatizar ou padronizar esta questão. A OAB? Nenhum. Isso aí, eu acho que a própria sociedade, ela vai identificar a necessidade e vai procurar o órgão para ver qual que é o padrão e forçar e estimular o órgão governamental a se preparar, a dar as respostas ali devidas". | 1 | - | 2 |
| | **T-2 Biometria** | **E05:** "a logística de emissão de certificação digital com biometria é ainda complexo. Coloca ainda que a identificação digital é mais segura e muito mais rápida, porque eu não preciso provar quem eu sou, só vai lá e identifica a digital, pois a tecnologia vem evoluindo... o equipamento para medir o calor, medir a pressão... ele mede algumas outras variáveis, mas o ser humano tem muita imaginação e cria diversos empecilhos que prejudicam a segurança, e acaba comprometendo o tripé, o que aumenta os riscos, considerando o nível de escolaridade no Brasil, sem infraestrutura adequada".<br>**E08:** "não houve uma evolução a respeito da certificação digital Biométrica. Ela é bastante onerosa". Afirma ainda ser bastante complicado a sua implantação, desde o aspecto legal ao operacional.<br>**E17:** Considera segura a utilização da biometria. Comenta ainda percebe que as pessoas já estão falando a respeito da biometria.<br>**E23:** Coloca que a identidade digital não é mais federal, mas estadual, o que abre brechas para ilegalidades. | 1 | 5 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | **T-3 Capacitação** | **E01:** Informa que foi promovido um encontro entre presidentes de comissões regionais da OAB. Entre os pontos levantados, a minimização dos impactos com relação ao peticionamento eletrônico e certificação digital. Mencionou ainda que existem as escolas exagenais (Exas) que são ramificações da OAB.<br>**E02:** afirma que a organização necessita de operacionalidade e investimentos para capacitar 757.000 advogados.<br>**E03:** Afirma que precisa de áreas capacitadas de suporte, bem dimensionadas, para atender um volume de usuários. Para tanto, precisa-se resolver este problema de forma inteligente. O entrevistado comenta que os parceiros, vinculados a organização, devem se unir para medir esforços nessa corrente.<br>**E05, E08 e E11:** Corroboram que é necessária uma sensibilização nesse processo de adaptação no uso da certificação digital.<br>**E05:** Coloca que alguns usuários mais diferenciados, não necessitam capacitação, pois já são acostumados a mexer com tecnologia.<br>**E08:** Coloca que é complicado inclusive estar orientando passo a passo porque dependendo do dispositivo, dependendo da mídia, dependendo da AR que for acionada o caminho é diferente, então e esse caminho toda hora tem novidade, enfim, é um problema importante a ser solucionado para massificar sem resolver isso acredito que a gente vai ter alguma dificuldade em desdobrar o que a gente vê hoje na parte de pessoa jurídica porque é um público bem especifico e focado naquilo então é mais estável, ele já está meio que preparado quando a gente coloca ai e dá um salto para universo de pessoa física (mesmo parceiros) vemos aí riscos e dificuldades.<br>**E10:** Afirma que são feitas reciclagens com agentes, principalmente quando alguns deles fazem perguntas básicas. "Isso é lição de casa". Alega que a capacitação é um tanto falha, muito ampla. Os agentes treinados em palestras são melhores do que os que fazem ensino à distância. Afirma que o treinamento não pode parar. | 5 | - | 5 |
| | **T-4 Criptossistema** | **E27:** "A ICP-Brasil é um criptosistema para uso da sociedade civil. Ai teria que fazer uma distinção entre redes fechadas e redes abertas. Ela é um criptosistema para ser usado onde as pontas se conhecem, então nós usamos algoritmos e padrões abertos, universalmente conhecidos pela sociedade. São lógicas completamente diferentes". | - | - | 2 |
| | **T-5 Desdobramentos da tecnologia** | **E08:** "o tipo de serviço é compatível com aquele nível de autenticação então se eu estou falando de autenticação desse tipo isso pode me permitir ceder pra ele um acesso a uma série de informações particulares que ele fez uma autenticação, mas talvez não uma alteração que pode gerar um desdobramento ai nesse caso eu precisaria de um nível mais forte de autenticação. Tem que ter um estudo para cada serviço de acordo com o tipo de | 1 | - | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | | autenticação que a gente vai disponibilizar". Coloca ainda que para você ter uma autenticação com biometria você está falando de ter um repositório que envolve toda uma logística de segurança para você ter um ambiente seguro, tem que ter toda uma política de rede para garantir a segurança de que aquilo não vai ser interceptado, que a princípio isso foi talvez o grande calo que o próprio ITI atravessou que era o meio de autenticação da biometria bastante onerosa ainda, tem todo o desdobramento. "Mesmo na parte operacional é bastante pesado, então quando eu estou falando daquela mídia biométrica que está no cartão, eu preciso de um repositório eu tiro uma série de variáveis quando eu estou falando de "ok" não tem uma mídia é um dado biométrico". | | | |
| | **T-6 Dificuldade de instalação** | **E02, E03, E04, E05 eE09:** comentam que há uma dificuldade em baixar a cadeia de certificados ICP-Brasil e que não há um suporte efetivo nesse aspecto.<br>**E02: "**Eu entendo que a certificação é válida ela traz segurança, que *login* e senha não trazem, no entendo é muito difícil trabalhar eu não consegui ainda baixar a cadeia toda, deu trabalho. O ajuste nos tribunais deveria ser mais simplificado e isso é um entrave".<br>**E03:** Coloca que o mercado passa a desacreditar se a tecnologia passar a dar problemas.<br>**E09:** Coloca que quando os usuários do sistema tinham dificuldades com a instalação da cadeia de certificados, havia um repúdio muito grande ao uso do sistema, que acabou sofrendo alterações ao longo do tempo com o apoio de profissionais da área que identificavam as dificuldades, tornando-o hoje mais bem aceito pelo público. | 8 | - | - |
| | **T-7 Ferramenta amigável** | **E07:** "todo o trabalho dos atributos é no sentido de oferecer a ele a facilidade de uso, dos hospitais e clínicas, mas civil também".<br>**E14:** Coloca que a dificuldade de utilizar, faz com que as pessoas resistam.<br>**E16:** "Temos dificuldade na utilização, mas não é a certificação digital, o problema é técnico, a atualização automática às vezes faz parar de funcionar, o sistema é muito volátil. O usuário tem dificuldade. Isso não é da AC. Tem a ver com o ambiente. Além disso, precisa estar compatível com os programas dos computadores".<br>**E20: "**os advogados têm dificuldade com a instalação e temos problemas com uma interface nada amigável". | 3 | 1 | 2 |
| | **T-8 Infraestrutura ICP e Brasil** | **E01 e E05:** afirmam que a infraestrutura brasileira, no que se refere ao investimento em energia, em computadores, internet para toda a dimensão geográfica do Brasil, é atrasada. Isso dificulta a popularização da certificação digital para o cidadão.<br>**E03:** Coloca que a infraestrutura é deficiente para emissão de certificados em massa.<br>**E04:** Coloca que a universalização dos certificados digitais no país, ela demanda infraestruturas que por um conjunto de razões estão atrasados. | 7 | 1 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | **E09:** Coloca que a infraestrutura de certificação no Brasil não é simples. | | | |
| | **T-9 Interoperabilidade** | **E01, E02, E03 e E14:** comentam que os sistemas devem se comunicar para proporcionar mais agilidade aos processos e qualidade nos serviços prestados. Dessa maneira, eles esperam que sejam feitos esforços na conversão para um sistema único.<br>**E02: "**Existem 45 sistemas rodando de processos eletrônicos, alguns não se comunicam, ou na migração, não se integram. Existe uma proposta de um processo de integração disso tudo, partindo da plataforma do TJE, ao que parece ele não está caminhando (seja por infraestrutura ou os processos dos tribunais) e está tirando muita gente do mercado sem necessidade".<br>**E03:** Cita que um certificado é reconhecido em computador, no entanto, em alguns casos, não é reconhecido em outro.<br>**E05 e E08:** Comentam que os caminhos para baixar a cadeia de certificados não é sempre o mesmo.<br>**E05:** "O caminho que vem sendo percorrido e que se tem em vista na padronização do uso da tecnologia para a ISO é fantástica. Não vai ser por falta de padronização, o problema é, novamente, a logística, a estratégia para capacitar 200 milhões de habitantes". | 7 | 3 | 1 |
| | **T-10 Logística de emissão/ reemissão do certificado** | Foi considerada por muitos dos entrevistados como o aspecto frágil para a evolução da certificação digital. Eles comentaram que as Autoridades Certificadoras (AC), em geral, não se planejam para uma emissão e remissão de certificados em massa. Além disso, tem uma estrutura de emissão burocrática.<br>**E03:** Coloca que o processo de emissão de certificados é muito lento e burocrático. Destaca que existe uma AC vem investindo em logística de emissão de certificados mais eficiente, com um processo menos burocrático. Ou seja, vislumbra-se um cenário de progresso nesse aspecto.<br>**E05:** Percebe que o grande problema para a utilização em massa do certificado digital é a logística de emissão. Coloca como expectativa que efetivamente, a certificação digital ela venha a ser massificada, que o, o cidadão venha a ter o seu certificado digital, principalmente em função do RIC e, pela própria evolução natural das aplicações que estão cada vez pedindo um suporte de segurança maior, que a certificação vem trazer. E ressalta novamente a questão da logística de emissão dos certificados que é o maior problema percebido pelo entrevistado e que se o governo eletrônico não acompanhar, será emitido certificado por emitir, pois não terá uso.<br>**E16:** Apresenta um exemplo com relação a dificuldade na emissão de certificados: "se o usuário demora 3 meses para receber o certificado, então, supondo que o certificado tenha sido roubado ontem, e o usuário necessita realizar operações mais complexas, como assinar | 6 | 1 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | | e tomar decisões, essa logística de emissão torna-se um gargalo". | | | |
| | **T-11 Novas aplicações da tecnologia** | **E03, E04, E05, E07 e E08:** corroboram que há a necessidade de ampliar o uso da certificação digital em determinados serviços, contudo, não veem necessidade de todo e qualquer serviço incluir certificação digital. Além disso, o entrevistado E04, afirma que "é preciso fazer uma análise crítica de quais são os serviços que efetivamente empregam o uso da certificação digital".<br>**E03:** "A expectativa é que com a certificação digital o cidadão tenha condições de ele próprio fazer a petição. Embora, a gente saiba que a OAB tem restrições aos postulantes. [...] mas, nos juizados e no judiciário, tem uma lei que autoriza o acesso ao judiciário sem este custo com o advogado".<br>**E05:** Dialoga a respeito de aplicações que estão dando certo, às quais denomina serviços estruturantes, e questiona sobre onde estão os demais, o governo eletrônico, não é, todo o benefício que se poderia vir a ter essa camada mais de segurança, ainda é muito pouco em todo o país. Comenta ainda que o ITI não tem como estimular tanto a criação de aplicações, mas a própria sociedade, com atrativos da tecnologia.<br>**E07:** "É importante que o cidadão tenha um cartão de saúde com certificação digital que respalde a segurança em todas as esferas que a certificação digital proporciona (integridade, não repúdio, etc.). Mas vale ressaltar que para os médicos é preciso que as instituições deem condições de fazer o registro no cartão do paciente. O futuro dos médicos, principalmente em hospitais é migrar totalmente para certificação digital, porque está todo mundo querendo sair do papel. Se tem o desejo, o sonho, de que 400 mil médicos estejam todos com as carteiras de identidade do médico (com certificação digital) e manuseando estes processos de forma eletrônica no consultório ou no hospital, pelo menos na região Sul e Sudeste, porque é a região mais informatizada do país, 72% dos médicos estão nesta região, ou seja, 2/3 dos médicos estão na região Sul e Sudeste. E uma pesquisa que já temos, 2 ou 3 anos atrás, é que 90% destes médicos usavam computadores em casa ou nos hospitais".<br>**E08:** "À medida que eu tenho serviço eu atenda aquele grupo que tem demanda efetiva e gradualmente eu vou estendendo o setor até chegar num ponto que eu tenha sido basicamente massificado, pelo menos para as pessoas que mexem com operações mais críticas". | 1 | 2 | 5 |
| | **T-12 Número de aplicações com utilização da tecnologia** | **E05:** Coloca que o mais crítico nesse momento é, não é nem tanto ao não uso, que é uma vez que tem valor legal, que garante não repúdio, que as aplicações estão indo devagarzinho, mas estão se encaminhando para ser certificação digital, mas a logística de emissão. | 4 | - | 2 |

| | | | | | |
|---|---|---|---|---|---|
| | | **E25:** "foi levantada a questão de como convencer a Pessoa Física para utilizar certificação, uma vez que são poucas aplicações para utilização". | | | |
| | **T-13 Número de certificados emitidos** | **E12:** Coloca que a demanda ainda é pequena.<br>**E27:** "Este ano nos dois primeiros bimestres a OAB teve um nº de emissões de CD como nunca vi, houve o amadurecimento desse setor e vê a oportunidade de usar essa ferramenta". | 1 | 1 | - |
| | **T-14 Ponto de venda** | **E20:** "O atendimento feito pelas AR's são péssimos. [...] os agentes de registros não são capacitados para atender".<br>**E26: "**O modelo de negócios está mudando, as configurações estão mudando. A questão do *delivery* é a mais comum, é agendado um dia para chamar os clientes para emitir certificado. Isto não é posto provisório, isso não é instalação técnica, isso não é ponto de venda, isso não é nada. No caso da SERASA ele entrega o certificado pré-datado. Ele tem um prazo de 3 dias pra aprovar este certificado. Ele tem esse prazo para reavaliar a documentação. Emite na hora e depois confere. A regra é, você tem que ter duas pessoas conferindo, então o que a SERASA nos outros casos, se você faz isso com a outra AC, ele confere e ele não emite o certificado, porque não pode emitir dali. Então você tem que ter um outro modelo de negócio. Entreguei, conferi, toma aqui o seu cartão, então agora você vai esperar receber um e-mail, você vai clicar no seu e-mail, ai que você vai gerar o certificado. Mas ai o cidadão vai dizer: "mas daí tem que instalar *drivers*, leitora, cartão… não sei como é que eu faço", então não sabe fazer, então cada um tem um jeito de fazer negócio. Então, tem outros que falam, não, eu só atendo na minha instalação técnica, porque aqui eu tenho uma pessoa treinada, que vai fazer para você, e você vai sair daqui com o seu cartãozinho, mesmo que isso, que é um modelo que está começando agora em função das fraudes, começando a valer, você vai num ponto de venda desse, apresenta os seus documentos, o carinha lá pega os seus documentos, confere, assinou, ele digitaliza aquilo e manda pra um outro lugar, em outro Estado. Por isso, esse conceito de instalação técnica muda muito". | 1 | - | 1 |
| | **T-15 Resistência ao uso** | **E06:** Coloca que no início havia resistência ao uso, hoje não, as pessoas já tem consciência da importância. "A palavra certa é sensibilização e não capacitação, pois esta soa como obrigação. Para o cidadão sobre a certificação digital hoje é de que sou obrigado. Mas quando ele conhece as vantagens/facilidades, percebe as aplicabilidades, agilidade, isso começa a pesar. Infraestrutura ainda não está adequada".<br>**E07:** Coloca que alguns setores como hospitais tem resistência ao uso da certificação, e utilizam outro tipo de tecnologia, e acabam tendo o problema de validade jurídica. Mas na | 4 | - | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | área médica em si, há uma percepção de que não há mais retorno. "Há uma crise, no momento, na medicina, uma transição não só dos processos de registro eletrônicos, mas da própria maneira de se fazer medicina. Então resistência existiu, vem diminuindo e é um processo irreversível, que com as novas gerações de profissionais vai acabar". | | | |
| | **T-16 Tecnologia imposta** | **E05:** Em relação a tecnologia imposta, coloca que acaba sendo natural, pois surge de legislações, necessidades que a legislação cria e também como uma oportunidade de negócio, como no caso das carteiras estudantis com certificação digital para compra de ingressos na Copa do Mundo.<br>**E18:** Coloca que é necessário trabalhar para a mudança, cultura da obrigatoriedade para a cultura de benefício que a certificação digital possibilita.<br>**E27: "**Seja do ponto de vista relacional, seja do ponto de vista econômico, a CD ainda traz polêmica, podemos discutir vários aspectos, são cronogramas de obrigatoriedade. Todas essas aplicações, elas estão inseridas em cronogramas de obrigatoriedade. O status, ele impõe. Por si só, já gera impacto. Ou seja, NF-e, a RF com o e-CAC, [...], teve um piloto e um ano depois teve um cronograma de obrigatoriedade. Inicialmente com alguns setores, depois cronograma foi se estendendo. Então isso é de certa forma antipático, mas é de certa forma compreensível, porque a cultura do nosso país, se você não impõe, o SPED, se não tivesse sido imposto, não ia sair nunca. Quer dizer, você tem algumas elites, algumas empresas de ponta, que iam vislumbrar, que iam usar, mas a grande massa não ia usar. A gente tem que entender as medidas de certa forma, duras. Se não é essa pressão, a sociedade, ela vai se postergando, vai atrasando, o que inviabiliza". | 2 | 1 | 8 |
| | **T-17 Tempo de emissão/ renovação do certificado** | **E26:** Coloca que é preciso estipular um tempo médio para a emissão dos certificados. | 3 | - | 1 |
| **Territorial TR** | **TR-1 Aquisição de certificados de fora do país** | **E23:** "a identificação de pessoal ela não é mais federal ela é estadual. E cada estado tem sua própria regra. [...] E quantas identidade servem para dar conta de coisas que são ilegais? E com conhecimento de quem está no sistema. Então, unificar isso é complicado. Tem que vencer interesses [...]. E uma hora vai estourar, e ai quem faz certificação, vai dizer, "olha eu faço uma certificação muito boa fora do Brasil", e ai vai todo mundo correr pra lá". | 1 | - | - |
| | **TR-2 Certificação do passaporte** | **E 24:** "o Itamaraty quer ficar com a questão do passaporte para ele. Querem fazer uma Autoridade Certificadora. Eles já são AR do SERPRO. Isso pode gerar uma internacionalização, uma outra realidade. Na área de certificação digital isso está sendo referência". | - | 1 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | **TR-3Internacionalização** | **E25:**Comenta que a Europa quando olha para o Brasil: Brasil é o futuro. Para eles já não existe América latina, existe Brasil e outros ao redor. “Essa questão da segurança eletrônica do Brasil é fundamental para que todo o mundo tenha uma percepção muito mais positiva do Brasil. A implantação da assinatura eletrônica na China, é muito complicada, mas um ponto importante é servir de ponte entre China e Brasil, e esta ponte necessita de segurança eletrônica. Foi tentado fazer esta relação com Portugal há alguns anos, esta parceria, por parecer mais fácil pelas relações, nosso certificado ser aceito lá e o deles aqui, mas não teve negociação, não foi aceito. No último momento Portugal desistiu. “Se eu fosse presidente da Casa Civil, faria uma aposta brutal na certificação digital [...]. Para que o Brasil se torne uma potência mundial, eu preciso fazer negócios seguros com o Brasil”.<br>**E27: “**O Brasil, ele tem um modelo, eu diria muito *sui generis*, quer dizer, nós construímos um caminho nosso. [...] Nós sempre trabalhamos muito pouco, a relação com outros países, por quê? O desafio de construir uma infraestrutura no Brasil são tão grandes, tínhamos tanta coisa para fazer, ainda temos tantas coisas, que não tinha sentido a gente pensar: “ah, vamos fazer alguma coisa com Portugal, por exemplo, que nós trocamos muito documento civil”, temos muito comércio [...] onde tem comércio, onde tem relação civil, tem papel, poderíamos ter trabalhado, tentamos um época, mas… o MERCOSUL, mas… com tanto desafio, com tanta coisa a percorrer que era um esforço que não valia a pena, por quê? Porque o Brasil acabou desenvolvendo um sistema escorado nas regras e nos padrões universais, não inventamos nada, todos os padrões ICP-Brasil são padrões universais, emitidos por organismos internacionais, padrões abertos, não patenteados, ou seja, o que preserva a disputa concorrencial, quer dizer, ninguém é dono de padrão nenhum, quem quiser implementar uma solução conhecida, pode implementar, mas o nosso caminho foi muito específico. [...] na verdade, eu diria que até na Europa, até com os problemas de estagnação econômica, [...] ela hoje se volta muito para *business* para o que ela pode fazer com o Brasil, e porque essa coisa tomou rumo e dimensões que você não encontra em nenhum país, em nenhum país europeu. A começar pelo nosso padrão, talvez só Alemanha e Coréia tenham um padrão hierárquico baseado numa raiz única, governamental, como tem o Brasil. Boa parte dos países, por exemplo, os EUA, não tem este tipo de desenho hierárquico, como tem a ICP-Brasil”. | - | - | 2 |
| | **TR-4 Migração de certificadoras de outros países** | **E25:**Comenta que se as certificadoras de outros países não tem que pagar, é um negócio fantástico, elas estão vindo pra cá. | - | 1 | 1 |

Fonte: o autor.

A partir da análise da Tabela 2, foi possível identificar quais as temáticas obtiveram maior percepção de impacto da tecnologia, seja positivo, negativo ou mesmo as temáticas que são apenas comentadas, estas últimas, principalmente representam ações indiretas à tecnologia, mas que foram possíveis através dela.

As cinco temáticas mais discutidas pelos especialistas foram: Segurança tecnológica – jurídica (15), Desmaterialização (14), Modelo de negócio adotado (13), Acessibilidade (13) e Custo do certificado (12).

Na sequência serão discutidas as temáticas citadas por mais de cinco entrevistados e analisadas suas relações com demais temáticas e dimensões.

### 4.4.1 Benefícios da Certificação Digital no Brasil a partir da percepção de especialistas

Foram identificadas como benefícios ou potencialidades da certificação digital (Tabela 3), a partir da percepção dos especialistas, as seguintes temáticas: A-1 Desmaterialização, L-13 Segurança tecnológica – jurídica, P-5 Interorganizações e S-1 Acessibilidade.

**Tabela 3: Benefícios da certificação digital ICP-Brasil**

| Dimensão | Temática | Frequência Percepção Positiva |
|---|---|---|
| **Ambiental A** | A-1 Desmaterialização | 9 |
| **Legal L** | L-13 Segurança tecnológica - jurídica | 9 |
| **Política P** | P-5 Interorganizações | 7 |
| **Social S** | S-1 Acessibilidade | 7 |

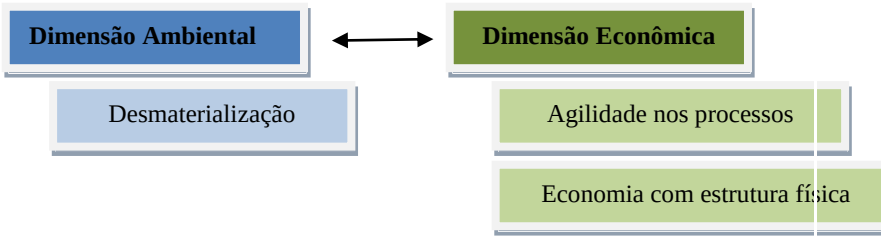
Fonte: o autor

As temáticas: desmaterialização e segurança foram citadas por nove entrevistados. A maioria deles reconhece que a questão da segurança é o objetivo fundamental da existência dessa tecnologia, neste sentido, entende-se que ela está cumprindo seu papel.

Em relação à desmaterialização, apesar de ter sido citada por nove entrevistados, um deles considerou que ela não está ligada diretamente a certificação digital, mas sim os sistemas computacionais.

Afirma que a certificação digital motiva a utilização desses sistemas, pois o usuário se sente seguro e não imprime no papel, o que acaba impactando na economia de papel. Neste sentido, essa temática está relacionada também às temáticas: agilidade nos processos e economia com estrutura física, ambas da dimensão **Econômica** (Figura 20).

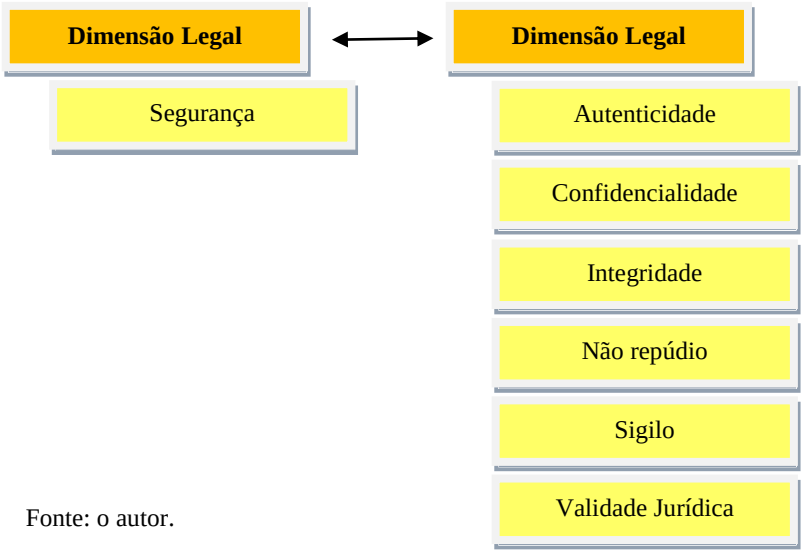
**Figura 20: Relação entre dimensões ambiental e econômica**




Fonte: o autor.

A partir das colocações dos entrevistados, é possível perceber que a questão da segurança está ligada ainda com a validade jurídica e intimamente ligada a autenticidade, confidencialidade, integridade, não repúdio e a privacidade, todas presentes na dimensão **Legal** (Figura 21).

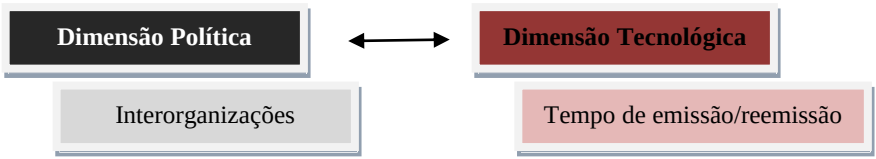
**Figura 21: Relação entre as temáticas da dimensão legal**




Fonte: o autor.

A temática interorganizações foi citada por sete entrevistados, os quais argumentam que as parcerias permitem uma maior disseminação da tecnologia e que os convênios firmados, na maioria das vezes, favorecem a adoção dos certificados, apesar de que um dos entrevistados colocou que tais convênios acarretam em uma demora na sua emissão, pois se há um convênio, não há porque adquirir certificado de outra AC (Figura 22).

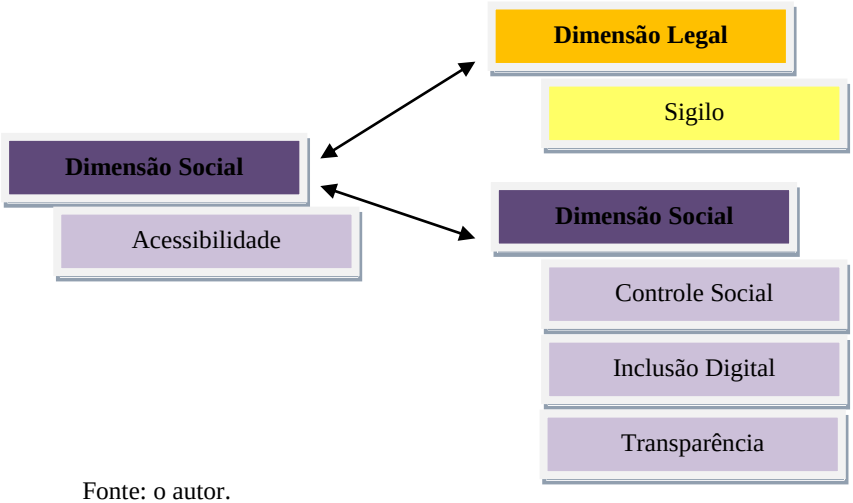
**Figura 22: Relação entre dimensões política e tecnológica**




Fonte: o autor

A temática acessibilidade foi apontada também por sete entrevistados, onde todos corroboram para a ideia de que a certificação digital permitiu maior acesso às informações. Esta temática estaria ligada às temáticas: sigilo, transparência, controle social e inclusão digital, ou seja, tem relação com as dimensões **Legal e Social**(Figura 23).

**Figura 23: Relação entre dimensões social e legal**



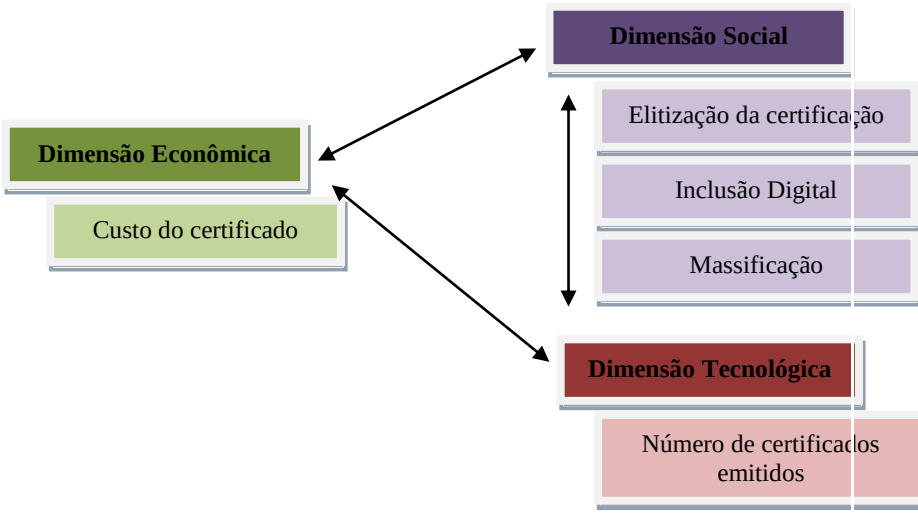

Fonte: o autor.

Desta forma, observa-se que as dimensões com impacto positivo, de acordo com a percepção dos especialistas são não só as dimensões Ambiental, Legal, Política e Social, mas ainda a dimensão Econômica, respectivamente.

### 4.4.2 Fragilidades da Certificação Digital no Brasil a partir da percepção de especialistas

Em relação às fragilidades da certificação digital apresentadas na Tabela 4, observa-se que o custo do certificado apresenta-se como o maior impacto negativo, principalmente em relação à adoção da tecnologia e às poucas aplicações/sistemas que a utilizam. Esta temática faz parte da dimensão Econômica e tem relação com as temáticas: Elitização da certificação, Inclusão digital, Massificação da tecnologia e ainda número de certificados emitidos, ou seja, se relaciona com as dimensões **Social e Tecnológica** (Figura 24).

**Figura 24: Relação entre dimensões econômica, social e tecnológica**

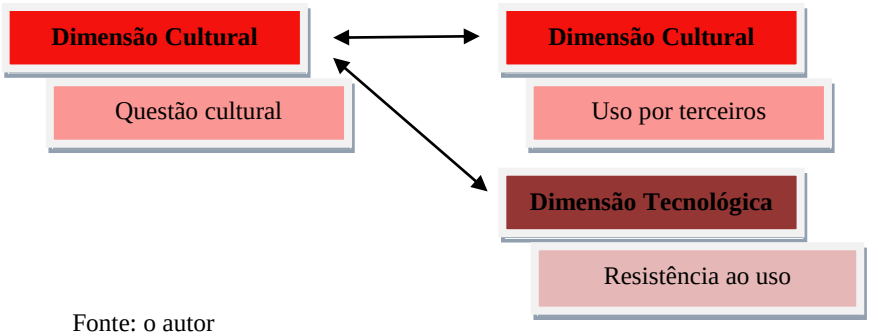



Fonte: o autor.

A temática questão cultural, presente na dimensão cultura foi apontada por sete entrevistados como um ponto negativo, principalmente porque muitas pessoas ainda não se adaptaram a leitura

digital e acabam imprimindo os documentos para realizar a leitura (E01), além do "Medo" do novo, do que é desconhecido; do processo de transição para a nova tecnologia acarretar inicialmente em mais "trabalhos". Pelos depoimentos dos entrevistados esta temática se relaciona com a temática: uso por terceiros, também da dimensão **cultural** e resistência ao uso, da dimensão **tecnológica**(Figura 25).

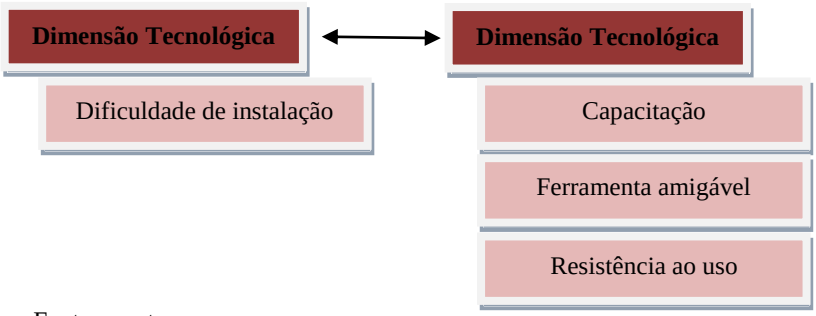
**Figura 25: Relação entre as temáticas da dimensão cultural e tecnológica**




Fonte: o autor

A temática dificuldade de instalação, apontada por oito entrevistados, uma vez que alegam que é muito difícil instalar a cadeia de certificados e dificilmente há uma capacitação para tal, ou seja, esta temática está relacionada com capacitação, ferramenta amigável e resistência ao uso e consequentemente às dimensões **Social e Tecnológica** (Figura 26).

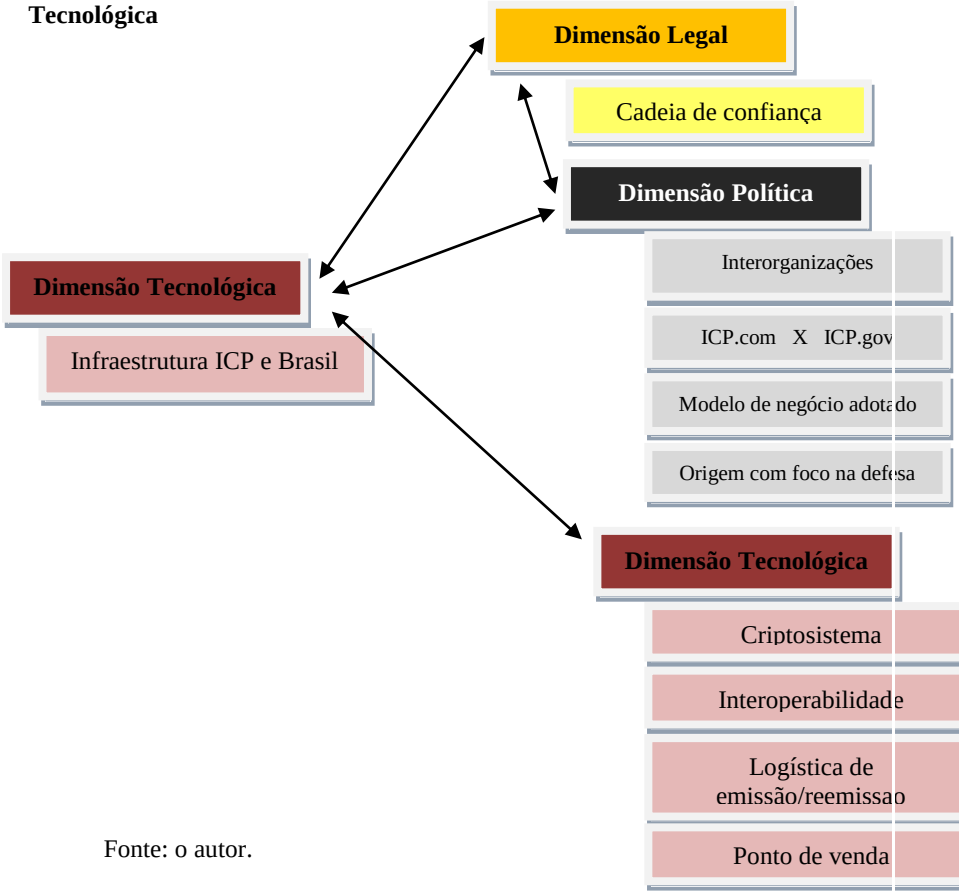
**Figura 26: Relação entre as temáticas da dimensão tecnológica**




Fonte: o autor.

Em relação à temática Infraestrutura ICP e Brasil, comentada por sete especialistas, foi colocada uma deficiência seja da própria estrutura ICP e mais ainda da estrutura de longo alcance social e tecnológico (no que se refere ao investimento em energia, em computadores, internet para toda a dimensão geográfica) no Brasil, como questionou um dos entrevistados: Como alcançar, por exemplo, a população ribeirinha que nem mesmo tem saneamento básico e energia? Esta temática está relacionada às temáticas Cadeia de Confiança, ICP.com *versus* ICP.gov, Modelo de negócio adotado, Origem da tecnologia com foco na defesa, Criptossistema, Logística de emissão/ reemissão do certificado, Ponto de venda e Interoperabilidade, ou seja, está relacionada às dimensões **Legal, Política e Tecnológica** (Figura 27).

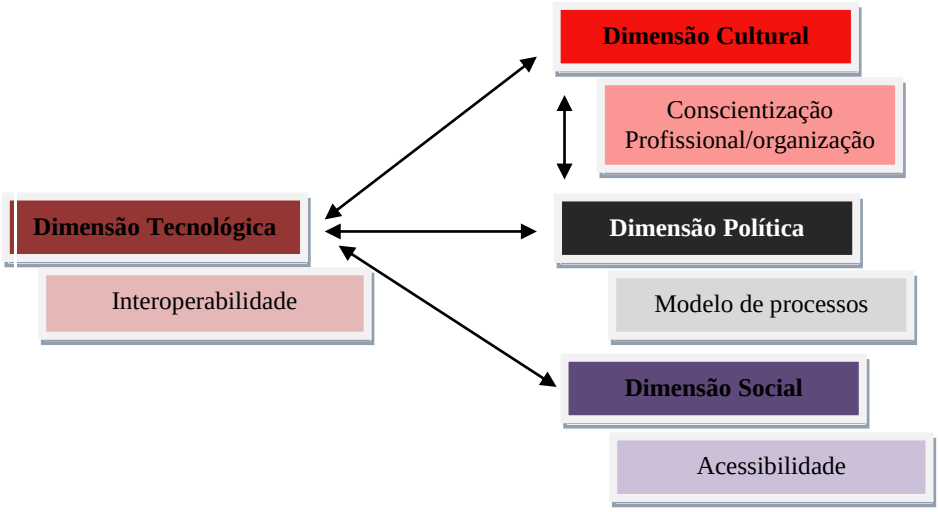
**Figura 27: Relação entre as dimensões tecnológica, Legal, Política e Tecnológica**




Fonte: o autor.

A temática Interoperabilidade, diz respeito às questões de falta de padronização de sistemas e bases de dados, uma vez que na maioria dos casos cada unidade possui sistemas próprios que não são interligados, como relatam os entrevistados E01, E02, E03 e E14 sobre a falta de integração entre os sistemas, ou seja, os sistemas devem se comunicar para proporcionar mais agilidade aos processos e qualidade nos serviços prestados. Ressalta-se que esse entrave não é ocasionado pela certificação digital, no entanto, houveram expectativas de que, com a implantação da certificação digital, houvesse uma maior mobilização para integração dos sistemas organizacionais. Neste mesmo sentido, ainda foi explanado sobre a falta de padronização dos *softwares* dos próprios computadores, como comenta o entrevistado E03, que o certificado é reconhecido em computador, no entanto, em alguns casos, não é reconhecido em outro. Esta temática está relacionada às temáticas: Conscientização do usuário profissional/ organizacional, Modelo de processos e Acessibilidade, e consequentemente está ligada às dimensões **Cultural, Política e Social** (Figura 28).

**Figura 28: Relação entre as dimensões tecnológica, Cultural, Política e Social**

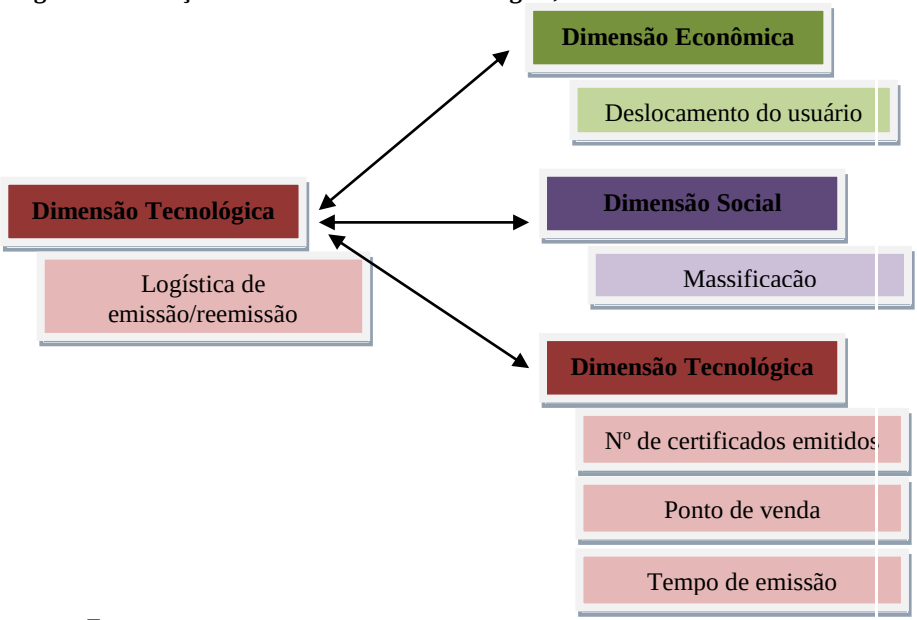



Fonte: o autor.

Em relação à Logística de emissão/ reemissão do certificado, alguns especialistas comentaram que este é um aspecto frágil para a evolução da certificação digital. Relataram que as ACs, em geral, não se planejam para uma emissão e remissão de certificados em massa, há uma falta de padronização do tempo de emissão e ainda apresentam uma estrutura de emissão burocrática. Como expõe, por exemplo, o entrevistado E15: "*Se o usuário demora três meses pra receber o certificado, então, supondo que o certificado tenha sido roubado ontem, e o usuário necessita realizar operações mais complexas, como assinar e tomar decisões, essa logística de emissão torna-se um gargalo*" (E15).

Por outro lado, o entrevistado E03 destaca que existe uma AC que vem investindo em logística de emissão de certificados mais eficiente, com um processo menos burocrático. O que demonstra um cenário de progresso nesse aspecto. Esta temática está relacionada às temáticas: Deslocamento usuário para emissão do certificado, Massificação, Número de certificados emitidos, Ponto de venda e Tempo de emissão/ renovação do certificado, ou seja, consequentemente, relacionada às dimensões **Econômica, Social e Tecnológica** (Figura 29).

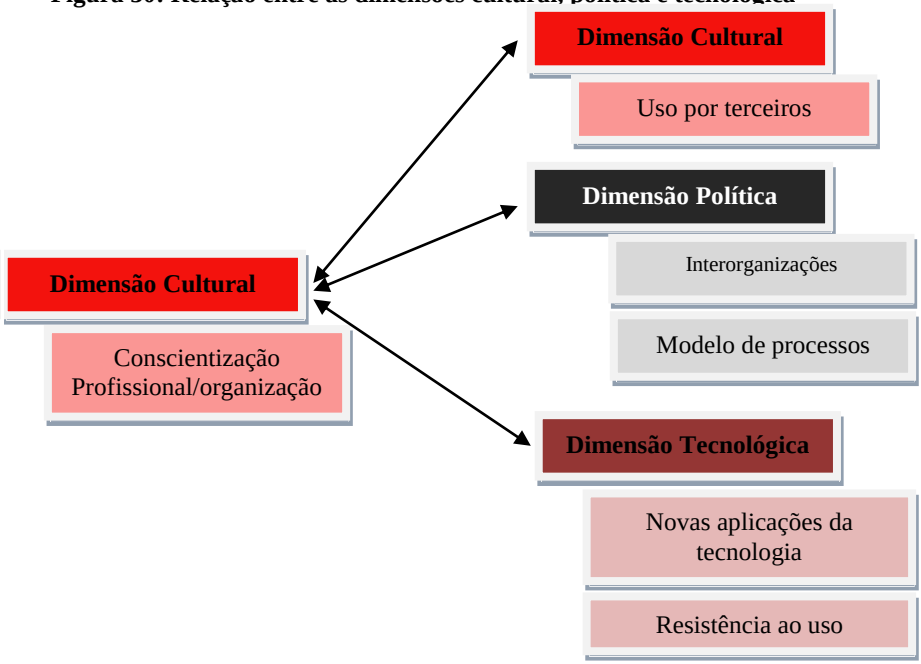
**Figura 29: Relação entre as dimensões tecnológica, econômica e Social**




Fonte: o autor.

Por fim, em relação à temática Conscientização do usuário profissional/ organizacional, foi relatado que muitos profissionais já entendem a importância da certificação digital, mas que a iniciativa privada ainda não possui interesse em desenvolver políticas e não se pode obrigar os profissionais a adquirir carteiras de classe com certificado, pois ainda tem um custo alto. Esta temática apresenta relação com as temáticas: Uso por Terceiros, Interorganizações, Modelo de processos, Novas aplicações da tecnologia e Resistência ao uso, ou seja, relacionada às dimensões **Cultural, Política e Tecnológica** (Figura 30).

**Figura 30: Relação entre as dimensões cultural, política e tecnológica**




Fonte: o autor.

**Tabela 4: Fragilidades da certificação digital ICP-Brasil**

| Dimensão | Temática | Frequência Percepção Negativa |
|---|---|---|
| **Econômica E** | E-3 Custo do certificado | 9 |
| **Cultural C** | C-4 Questão cultural | 7 |
| **Tecnológica T** | T-5 Dificuldade de instalação<br>T-7 Infraestrutura ICP e Brasil<br>T-16 Unificação/ Integração/ Adequação/ Padronização de sistemas/bases/ Interoperabilidade<br>T-8 Logística/ processo de emissão/ reemissão do certificado | 8<br>7<br>7<br>6 |
| **Cultural C** | C-3 Conscientização do usuário profissional/ organizacional | 6 |

Fonte: o autor.

Desta forma, observa-se que as únicas dimensões que não tiveram relação direta com as temáticas que mais apresentaram percepções negativas foram a Ambiental e a Territorial.

Percebe-se ainda que as temáticas e consequentemente, nem mesmo as dimensões se repetiram como positiva e negativa ao mesmo tempo.

## 4.4 CONSIDERAÇÕES PERTINENTES AOS RESULTADOS

Em resumo, utilizou-se da visão sistêmica para identificar os atores envolvidos com a certificação digital, bem como sua composição, estrutura, ambiente, mecanismos e ainda a fronteira e possíveis sistemas envolvidos. Como é um sistema complexo, não se conseguiu aprofundar o entendimento destes outros sistemas. Esta etapa foi imprescindível para a sequência do trabalho, que foi a identificação das temáticas levantadas pelos entrevistados.

As temáticas representam direta ou indiretamente os impactos percebidos pelos especialistas, refletindo no processo de adoção da tecnologia.

Ressalta-se que as diversas temáticas impactam e são impactadas por outras temáticas, seja relacionadas à própria dimensão, seja de

dimensões diferentes. A Figura 31 demonstra resumidamente as relações existentes nas temáticas apontadas positivamente.

**Figura 31: Relações das temáticas percebidas como positivas pelos entrevistados**


Fonte: o autor.

Por exemplo, a temática S-1 Acessibilidade, da Dimensão Social, está relacionada às temáticas L-13 Sigilo, da Dimensão Legal e ainda às temáticas S-7 Transparência e S-5 Inclusão Digital da mesma Dimensão Social, o que podemos considerar que se um indivíduo não possui acesso à computadores e/ou internet (infraestrutura Brasil), partes da Inclusão Digital, este indivíduo não tem acessibilidade às informações. Tais questões refletem a dificuldade de análise do impacto da certificação digital, por ser bastante complexo. Diversas dimensões sofrem pressões de diversas outras e muitas vezes ela não está nem mesmo ligada diretamente à certificação, mas ao ambiente onde ela atua.

## 5. CONSIDERAÇÕES FINAISE TRABALHOS FUTUROS

Esta dissertação objetivou analisar o impacto da certificação digital no Brasil a partir da percepção de especialistas sugeridos pela cúpula do ITI.

Considera-se que o referencial teórico de maneira geral e a metodologia utilizadas nesta pesquisa foram importantes para o alcance do objetivo proposto.

Percebe-se que as inovações tecnológicas têm impactado profundamente todas as áreas da atividade humana, moldando e redefinindo práticas, processos, transações, percepções, produtos, dentre outras questões. No ambiente organizacional, a adoção de uma nova tecnologia, pode definir seu sucesso ou fracasso, seja do ponto de vista de uma organização adotante, seja do ponto de vista do empreendedor desta nova tecnologia, uma vez que ela impacta direta ou indiretamente a estrutura organizacional, os processos de trabalho, a produtividade, a sustentabilidade e sua competitividade.

Compreende-se que cada inovação tecnológica se difunde a uma razão e a um ritmo diferentes em seus mercados potenciais, onde a vantagem advém de uma aprendizagem resultante de uma série de sondagens de mercado, e que a capacidade de absorver incerteza e antecipar oportunidades é maximizada por processos que aumentam a gama de possibilidades, onde se busca uma convergência de conclusões entre métodos diferentes, e que as mudanças sociais, econômicas, ambientais, culturais e tecnológicas têm impactado profundamente umas às outras, principalmente nos quesitos inovação e competitividade

Considerando que o poder de impacto de novas tecnologias não é contemplado em modelos de análise tradicionais, que incorporam as dimensões da complexidade do cenário de desenvolvimento tecnológico atual, optou-se por uma análise multidimensional, que contempla-se a maior gama de dimensões possível. Para tanto, optou-se pela combinação de diferentes abordagens que possam suprir possíveis lacunas existentes em cada uma, onde partiu-se do princípio do uso do pensamento sistêmico, que serviu de base para a identificação não somente dos atores, composição, relações, da certificação digital, mas também contribuiu para a definição das dimensões e temáticas para análise do impacto de sua adoção.

Desta forma, foram utilizadas as teorias de Mendes (2009), Angeloni (2002) e Marques (2008) para a delimitação das dimensões de análise, e para o entendimento dos atores e relações envolvidas com a

certificação digital ICP-Brasil optou-se pela visão sistêmica de Bunge (2003), que foi fundamental para esta pesquisa.

Esta pesquisa envolveu a realização de entrevistas para obtenção da visão de especialistas de vários setores (Justiça, Ministérios, ACs, Saúde, Sindicatos e Associações, Bancário, e do ITI), houve o levantamento de dados junto ao ITI e na internet (documentos e publicações científicas) para descrição do contexto da certificação digital.

A partir da análise das 27 entrevistas, pode-se identificar as temáticas e consequentemente as principais dimensões que apresentam potencialidades e fragilidades e suas relações umas com as outras.

De maneira geral, percebe-se que a certificação digital reduz distância física, evita fraudes, falsificações e possibilita que um maior número de serviços eletrônicos sejam realizados com segurança.

Embora não se tenham números que evidenciem a disseminação da certificação digital ICP-Brasil em relação às pessoas físicas, tem-se a evidencia de que isso ocorre com maior impacto nas pessoas jurídicas, principalmente devido às aplicações serem basicamente de governo neste sentido.

Considerando dimensão do território brasileiro, em relação a população e o número de empresas, entende-se que a tecnologia ainda não está consideravelmente difundida, apesar de seus benefícios potenciais.

Considerando que uma tecnologia tem sua difusão baseada na disponibilidade de aplicativos para seu uso, verificou-se, ao longo dos anos, o aumento da disponibilidade de aplicações que usam a certificação digital, que são eminentemente fomentadas por instituições governamentais. Ou seja, o governo é o maior fomentador da certificação digital ICP-Brasil, sendo responsável não apenas pelo seu fomento, como também pela sua regulamentação e auditoria. Neste sentido, ficou evidenciado também, a complexidade da análise da difusão/adoção já que envolve vários sistemas, como representado no início. Existe uma dependência declarada, como pode ser observado nas entrevistas.

Nesta pesquisa dois contextos são claramente percebidos, quais sejam, as organizações que adotam a certificação digital ICP-Brasil para agregar valor e as que apenas a utilizam por força da obrigatoriedade da mesma ou atividade específica.

Analisando as principais fragilidades declaradas pelos entrevistados, percebe-se que o custo do certificado ainda é um problema e que há ainda, uma preocupação com aspectos relacionados

ao número de aplicações, que é extremamente dependente de ações de governo e que o setor privado fica sempre à espera das iniciativas do governo.

Muitos dos entrevistados comentaram que, para a certificação digital ser disseminada efetivamente, é necessária uma campanha para a criação de aplicativos voltados para o cidadão, já que a ICP-Brasil tem sido disseminada não para o cidadão, mas primeiramente com foco empresarial.

Por fim, de maneira geral, foram identificadas diversas potencialidades promovidas pelo uso da certificação digital ICP-Brasil, dentre eles destacam-se, a segurança e validade jurídica, economia de papel, redução de custos com espaço físico e atendimento presencial, agilidade na tramitação de documentos, maior agilidade nos processos e mais transparência. Já em relação às fragilidades se destacam: o custo do certificado, a questão cultural, dificuldade de instalação; a infraestrutura brasileira (energia, computadores, internet, *drivers*, softwares compatíveis etc.); a falta de padronização.

## 5.1 TRABALHOS FUTUROS

Como trabalhos futuros sugere-se que seja realizada uma análise de cenários, com ferramentas próprias desta técnica, e ainda seja realizado um estudo com desenvolvedores de aplicativos de diversos seguimentos.

Sugere-se realizar um estudo mais aprofundado das relações dimensionais apresentadas neste estudo e para cada uma das temáticas apontadas.

A sequência desta pesquisa, é a aplicação de outros instrumentos de pesquisa, como questionários, que possam sanar as lacunas, portanto, foram desenvolvidos dois instrumentos de pesquisa (questionários) que tem objetivos distintos, construídos com base nos trabalhos de Mahmood e Soon (1991), Torkzadeh e Doll (1999), Maçada (2001) e Spohr e Sauvé (2003) e aplicados pelos membros do IGTI e também no site do ITI, mas que não fazem parte da presente pesquisa.

Além disso, nesta pesquisa analisou-se o impacto sobre o ponto de vistas de especialista, desta forma, recomenda-se realizar uma análise com base no usuário final. Também pode-se realizar a pesquisa com base em usuários de um aplicativo específico ou ainda por setor (jurídico, por exemplo).

## REFERÊNCIAS

AFONSO, A. et.al. **Manual de Tecnologias da Informação e Comunicação**. Lisboa: ANJAF, 2010.

ALMEIDA, M.de.S. FREITAS, C.R. SOUZA, I.M. de. **Gestão do Conhecimento para tomada de decisão**. São Paulo: Atlas, 2011.

ALONSO, L. B. N; FERNEDA, E; BRAGA, L. V. **Governo Eletrônico e Políticas Públicas**: análise sobre o uso da certificação digital no Brasil. Inf. &Soc.:Est., João Pessoa, v.21, n.2, p. 13-24, maio/ago., 2011

ANGELONI, M.T. **Organizações do conhecimento: infra-estrutura, pessoas e tecnologias**. São Paulo: Saraiva, 2002.

ANTONELLI, R.A. et.al. **Estado da Arte do impacto da Tecnologia da Informação nas organizações**: um estudo bibliométrico. Revista CAP, 2010.

ARAUJO, W.J.de. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento**. Brasília: 2009. Tese. Doutorado em Ciência da Informação. Universidade de Brasília, UNB.

BAREGHEH, A.; ROWLEY, J.; SAMBROOK, S. **Towards a multidisciplinary definition of innovation**. Management Decision, v. 47, n. 8, p. 1323-1339, 2009.

BARDIN, L. **Análise de Conteúdo**. Lisboa, Portugal; Edições 70, LDA, 2006.

BERELSON, B. **Content analysis in communication research**. New York:Hafner; 1984.

BERTALANFFY, L.V. **Teoria Geral dos sistemas:** fundamentos, desenvolvimento e aplicações. Petrópolis: Vozes, 2010.

BERTOL, V. R. L. **Uma proposta para a regulamentação da Certificação Digital no Brasil**. Tese de Doutorado. 2009. Faculdade de Tecnologia. Universidade de Brasília.

BESSANT, J.; et.al. **Managing innovation beyond the steady state. Technovation**, v. 25, n. 12, p. 1366-1376, 2005.

BONACELLI, M.B; ZACKIEWICZ, M; BIN, A. **Avaliação de impactos sociais de programas tecnológicos na agricultura do Estado de São Paulo**. Espacios, Caracas, vol.24, n.2, 2003.

BORGES, C. L. **Ferramenta de comunicação e acesso remoto a imagens médicas**. Dissertação de Mestrado. Faculdade de Engenharia Elétrica e de Computação. Universidade Estadual de Campinas. Campinas, 2003.

BORTOLI, D. L. **O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais**. Dissertação de Mestrado. Ciências da Computação. Universidade Federal de Santa Catarina. Florianópolis, 117 p., 2002.

BRAGA, L. V. **O impacto do governo eletrônico sobre a prestação de serviços públicos no Brasil**: aplicações da certificação digital. Univ. Gestão e TI, Brasília, v. 1, n. 2, p. 87-102, jul./dez. 2011.

BRASIL, BRASIL. Lei. **Lei Nº 10.973, de 02 de dezembro de 2004**. Brasília-DF: Senado, 2004.

BUNGE, Mario. **Emergence and convergence**: Qualitative novelty and the unity of knowledge. University of Toronto Press, 2003.

BURRELL, G.; MORGAN, G**. Sociological paradigms and organisational analysis**. London: Heinemann Education Books, 1979.

CASTELLS, M. CARDOSO, G. (Orgs.) **A Sociedade em Rede**: do conhecimento à acção política. Conferência. Belém (Por): Imprensa Nacional, 2005.

CELEPAR. **Nivelamento Teórico em Certificação Digital da CELEPAR para Profissionais em Informática.** Celepar Informática do Pará, 2007. Disponível em: http://www.frameworkpinhao.pr.gov.br/arquivos/File/Apostila_Certificacao_Digital_TEC.pdf. Acessado em: 08/12/2014.

CRESWELL, J.W. **Projeto de pesquisa**: métodos qualitativos, quantitativos e mistos. 3. ed. – Porto Alegre: Artmed, 2010.

CHRISTENSEN, C.M. **O Dilema da Inovação**: quando as novas tecnologias levam empresas ao fracasso. São Paulo: M.Books do Brasil, 2012.

DAVILA, T. EPSTEIN, M.J. SHELTON, R. **As regras da Inovação:** como gerenciar, como medir e como lucrar. São Paulo: Bookman, 2007.

DAY, G.S; SCHOEMAKER, P.J.H; GUNTHER, R.E. **Gestão de tecnologias emergentes:** a visão da Wharton School. Porto Alegre: Bookman, 2003.

DELIBERADOR, P. T. **Um componente computacional para auxiliar o desenvolvimento de uma assinatura digital no sistema de informações processuais.** Dissertação de Mestrado. Pós-Graduação em Engenharia de Produção. Universidade Federal de Santa Catarina. Florianópolis, 186 p., 2004.

DEMÓCRITO, R. **Brasil**: A ICP-Brasil e os Poderes Regulatórios do ITI e do CG. AR: Revista de Derecho Informático, 2005.

EID, N. L. M. **Avaliação do conhecimento e utilização da certificação digital em clinicas de radiologia odontológica**. Dissertação de Mestrado. Faculdade de Odontologia de Piracicaba, da Universidade Estadual de Campinas. Piracicaba, 2007.

ESPÍNDOLA, M.B. et.al. **Integração de Tecnologias de Informação e Comunicação no Ensino**: Contribuições dos Modelos de Difusão e Adoção de Inovações para o campo da Tecnologia Educacional. Rio de Janeiro: UFRJ-RELATEC, 2010.

IGTI. **Avaliação de Impacto Socioeconômico da certificação digital no Brasil**: relatório de pesquisa. Florianópolis: IGTI-UFSC, 2013.

FARIAS, S.C. **Os benefícios das Tecnologia da Informação e Comunicação (TIC) no processo de Educação à Distância (EAD)**. Campinas: Rev. digit. bibliotecon. cienc. Inf, 2013.

FERNANDES, R.F. **Uma proposta de modelo de aquisição de conhecimento para identificação de oportunidades de negócios nas redes sociais**. Florianópolis: 2012. Dissertação. Mestrado em Engenharia e Gestão do Conhecimento. Universidade Federal de Santa Catarina, UFSC.

FERNANDEZ, B. O. **Proposta de um sistema eletrônico embarcado para fiscalização automática de veículos rodoviários de carga**. Tese de Doutorado. Departamento de Engenharia Mecânica. Escola de Engenharia de São Carlos da Universidade de São Paulo. São Paulo. 2010.

FRANTZ, M.B.F. **Criação e compartilhamento de conhecimento artístico e cultural em ambiente virtual interativo**. Florianópolis: 2011. Tese. Doutorado em Engenharia e Gestão do Conhecimento. Universidade Federal de Santa Catarina, UFSC.

FREITAS, H. RECH, I. **Problemas e ações na adoção de novas tecnologias de informação**. Rio de Janeiro: RAC, 2003.

GERHARDT, T.E. SILVEIRA, D.T. **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GIACOMINI Filho, G. et.al. **Difusão de inovações:** apreciação crítica dos estudos de Rogers. Porto Alegre: FAMECOS, 2007.

GIL, A.C. **Como elaborar projetos de pesquisa.** 5ª. ed. São Paulo: Atlas, 2010.

GUEDES, L.F. VASCONCELLOS, L. VASCONCELOS, E.P.G. de. **Adoção Organizacional de Inovações**: Um Estudo sobre a Decisão de Adotar a Tecnologia de Celulares de Terceira Geração. São Paulo: SEMEAD, 2008. Disponível em: http://www.ead.fea.usp.br/semead/11semead/resultado/trabalhosPDF/889.pdf. Acessado em: 10/01/2014.

ISHIKAWA, E. C. M. **Um modelo computacional para o funcionamento da assinatura digital no sistema de informatização processual**. Dissertação de Mestrado. Pós-Graduação em Engenharia de Produção. Universidade Federal de Santa Catarina. Florianópolis, 116 p., 2003.

ITI. Instituto Nacional de Tecnologia da Informação. Disponível em: <http://www.iti.gov.br/>. Acessado em: janeiro a agosto de 2013.

KERN, V. M. Plataformas e-gov como sistemas sociotecnológicos. In: ROVER, A. J.; GALINDO, F. (Orgs.). **O governo eletrônico e suas múltiplas facetas**. Série LEFIS, vol. 10. Zaragoza/Espanha: Prensas Universitarias de Zaragoza, 2010, p. 39-67.

KERN, V. M. (org) **Modsis 2009**: Caderno de anais da disciplina Modelagem de Sistemas. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. Universidade Federal de Santa Catarina, 2009.

KOBAYASHI, L. O. M. **Abordagem criptográfica para integridade e autenticidade em imagens médicas**. Tese de Doutorado. Escola Politécnica da Universidade de São Paulo. São Paulo, 2007.

LÈVY, Pierre. **As tecnologias da inteligência**: o futuro do pensamento na era da informática. Rio de Janeiro: Editora 34, 15. impressão, 2008.

LINS, B.F.E. **Comércio eletrônico, assinatura e certificação digital**. Brasília-DF: Câmara dos Deputados – Consultoria Legislativa, 2005.

MAÇADA, A. C. G. **Impacto dos Investimentos em Tecnologia da Informação nas variáveis Estratégicas e na eficiência dos Bancos Brasileiros**. Tese de Doutorado. 2001. Programa de Pós-Graduação em Administração. Universidade Federal do Rio Grande do Sul (UFRGS).

MARCIAL, E.C. GRUMBACH, R.J.S. **Cenários Prospectivos**: como construir um futuro melhor. Rio de Janeiro: FGV, 2008.

MARQUES, L.F.M. **Proposta de modelo de análise multidimensional para impactos de novas tecnologias**: interações entre nanotecnologia, economia, sociedade e meio-ambiente. Porto Alegre: 2008. Tese. Doutorado em Administração. Universidade Federal do Rio Grande do Sul, UFRGS.

MARTINEZ, R. H; PETRONI, B. C. A. **A Assinatura Digital e o Processo Judicial Eletrônico**: Um Estudo do Impacto da Revogação do Certificado Digital na Validade dos Atos Processuais. Acesso em: 10 de setembro de 2013. Disponível em: http://www.centropaulasouza.sp.gov.br/pos-graduacao/workshop-de-posgraduacao-e-pesquisa/anais/2010/Trabalhos/gestao-e-desenvolvimento-de-tecnologias-da-informacaoaplicadas/Trabalhos%20Completos/MARTINEZ,%20Ramses%20Henrique.pdf

MARTINI, R. S. **Tecnologia e Cidadania Digital**: ensaio sobre tecnologia, sociedade e Segurança. Rio de Janeiro: Brasport, 2008.

MARTINI, R. **Sigilo e Conhecimento**: Uma Introdução ao Problema. In: Panorama da Interoperabilidade no Brasil. Brasília, SLTI/MPOG, 2010.Disponível em: http://renatomartini.net/wp-content/uploads/2013/09/Sigilo_e_Conhecimento.pdf . Acessado em 04/06/2014.

MANZINI, E. **Design para a inovação social e sustentabilidade**: comunidades criativas, organizações colaborativas e novas redes projetuais. Rio de Janeiro: E-papers- UFRJ, 2008.

MENDES, J.M.G. **Dimensões da Sustentabilidade**. Revista das Faculdades Santa Cruz, v. 7, n. 2, julho/dezembro 2009. Disponível em: http://www.santacruz.br/v4/download/revista-academica/13/cap5.pdf. Acessado em: 26/02/2014.

MERINO RECINOS, O. E. **A importância do processo eletrônico, enquanto mecanismo célere de acesso à justiça, e diagnóstico de sua viabilidade em El Salvador**. Dissertação de Mestrado. Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2012.

MOECKE, C. T. **NBPKI - Uma ICP baseada em autoridades notariais**. UFSC: Programa de Pós-graduação em Ciência da Computação, 2011.

MOLLA, A. LICKER, P.S. **eCommerce adoption in development countries:** a model and instrument. Information & Manegement, v.42, n.6, Sep, p.877-899. 2005.

MORAES, Roque. **Análise de conteúdo**. Porto Alegre: Revista Educação, 1999.

MORETTO, L.A.M. GALDO, A.M.R..KERN, V.M. **Uma análise sistêmica sociotecnológica da engenharia de requisitos.** Florianópolis: R. Eletr. Bibliotecon. Ci. Inf., Florianópolis, n. esp., 2º sem. 2010.

MORGAN, G. **Paradigms, metaphors, and puzzle solving in organization theory**. Administrative Science Quarterly, v. 25, n. 4, p. 605-622, 1980.

MORGAN, Gareth. Paradigmas, Metáforas e Resolução de quebra-cabeças na Teoria das organizações. 1980. In: CLADAS, M.; BERTERO, C. O. (Coord.) **Teoria das Organizações**. São Paulo: Atlas, 2007.

MORITZ, G.O; MORITZ, M.O; PEREIRA, M.F. **Planejamento por cenários prospectivos**: referencial metodológico baseado em casos para a aplicação prática nas organizações. São Paulo: Atlas, 2012.

NAKAMURA, E.T; GEUS, P.L. de. **Segurança de Redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

NOBRE, L. F. **Certificação digital de exames em telerradiologia**: um alerta necessário. Radiol Bras., 2007.

NONAKA; I.; TAKEUCHI, H. **Criação de conhecimento na empresa:** como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Elsevier,1997.

NONAKA; I.; TAKEUCHI, H. **Gestão do conhecimento**. Porto Alegre: Bookman,2008.

OCDE. **Perspectivas da Tecnologia da Informação**: as tecnologias de comunicação e informação e a economia da informação. São Paulo: SENAC, 2003.

PRUSAK, L.MCGEE, J. **Gerenciamento Estratégico da Informação.** Rio de Janeiro: Campus, 1994.

REIS, D.R. dos. **Gestão da inovação tecnológica**. São Paulo: Manole, 2008.

ROCCHE, C. **Avaliação de impacto dos trabalhos de ONGs**: aprendendo a valorizar as mudanças. Edição adaptada para o Brasil pela ABONG. São Paulo: Cortez, 2000.

ROCKEMBACH, M. **A implantação da assinatura digital no Tribunal Regional Federal da Quarta Região**: perspectiva infocomunicacional. Dissertação de Mestrado. Programa de Pós-Graduação em Comunicação e Informação. Universidade Federal do Rio Grande do Sul. Porto Alegre, 133 p. 2009

ROGERS, E. M. **Diffusion of Innovation**. New York, USA: Free Press. 1995.

ROMANI, J. **Integração de serviços de relógio para Infraestrutura de Chaves Públicas**. UFSC: Programa de Pós-graduação em Ciência da Computação, 2009.

SABBAG, P.Y. **Espirais do Conhecimento**: ativando indivíduos, grupos e organizações. São Paulo: Saraiva, 2007.

SANTOS; A.M. dos. **Fatores influenciadores da adoção e infusão de inovações em TI.** In: Simpósio de excelência em gestão e tecnologia, 4., 2007, Resende, Pôster. Anais..., [S.I], 2007.

SANTOS, F.M.R. SOUZA, R.P.L. **O conhecimento no campo de Engenharia e Gestão do Conhecimento**. Belo Horizonte: Perspect. ciênc. inf., v. 15, n. 1, Apr. 2010.

SCHREIBER, G. et al. **Knowledge engineering and management**: the CommonKADS methodology. Massachusetts: MIT Press, 2000. 471 p.

SCHREIBER, G.; AKKERMANS, H.; ANJEWIERDEN, A.; HOOG, R; SHADBOLT, N.; VELDE, W. van de; and WIELINGA, B. **Knowledge Engnineering and Management:** the *CommonKADS* Methodology. MIT Press. Cambridge. Massachussets. 2002.

SILVA, E. L. e MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação** – 4ª. ed. rev. Atual. – Florianópolis: Laboratório de Ensino à Distância, 2005.

SILVESTRE, F. A. C. **A ilegitimidade constitucional crítica da Infraestrutura de Chaves Públicas Brasileira**: uma semiótica do poder. UFSC: Programa de Pós-graduação em Ciência da Computação, 2003.

SIMANTOB, M. LIPPI, R. **Guia valor econômico de inovação nas empresas**. São Paulo: Globo, 2003.

SQUIRRA, S. **Sociedade do Conhecimento.** In MARQUES DE MELO, J.M.; SATHLER,L. **Direitos à Comunicação na Sociedade da Informação**. São Bernardo do Campo, SP: Umesp, 2005.

STUDER, A. C. R. **Processo judicial eletrônico e o devido processo legal.** Dissertação de Mestrado. Programa de Mestrado em Ciência Jurídica. Universidade do Vale do Itajaí. Itajaí, p., 2007.

TIDD, J.; BESSANT, J.; PAVITT, K. **Gestão da Inovação**. 3. Ed. – Porto Alegre: Bookman, 2008.

TRIAS DE BES, F. KOTLER, P. **A bíblia da inovação**: princípios fundamentais para levar a cultura da inovação contínua às organizações. São Paulo: Leya, 2011.

TURBAN, E. RAINER, R.K. POTTER, R.R. **Administração de Tecnologia da Informação**: teoria e prática: Rio de Janeiro: Elsevier, 2005.

TURBAN, E. RAINER, R.K. POTTER, R.R. **Introdução a Sistemas de Informação**: uma abordagem gerencial. Rio de Janeiro: Elsevier, 2007.

YATES, B.L. **Applying Diffusion Theory**: Adoption of Media Literacy Programs in Schools. SIMILE, 2004.

# GLOSSÁRIO

**Assinatura Digital:** é um código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e-mail ou uma transação). Ela comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente (Disponível em: www.iti.gov.br).

**Autenticidade**: é a qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção (Disponível em: www.iti.gov.br).

**Autoridade Certificadora - AC**: é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada). Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada (Disponível em: www.iti.gov.br).

**Autoridade Certificadora Raiz - AC-Raiz**: é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. Ela também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e

normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil (Disponível em: www.iti.gov.br).

**Autoridade de Registro - AR**: é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota (Disponível em: www.iti.gov.br).

**Biometria**: é a ciência que utiliza propriedades físicas e biológicas únicas e exclusivas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz (Disponível em: www.iti.gov.br).

**Certificação Digital - CD:** É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora. É uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demanda identificação clara da pessoa que a está realizando pela intranet (Disponível em: www.iti.gov.br).

**Certificado Digital:** O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso. Na prática, ele funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora. Os certificados contêm os

dados de seu titular, como nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme especificado na Política de Segurança de cada Autoridade Certificadora (Disponível em: www.iti.gov.br).

**Certificado de Atributo**: Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos (Disponível em: www.iti.gov.br).

**Chave Privada**: Uma das chaves de um par de chaves criptográficas (a outra é uma chave pública) em um sistema de criptografia assimétrica. É mantida secreta pelo seu dono (detentor de um certificado digital) e usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente (Disponível em: www.iti.gov.br).

**Chave Pública**: Uma das chaves de um par de chaves criptográficas (a outra é uma chave privada) em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente. Dependendo do algoritmo, a chave pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a chave privada correspondente (Disponível em: www.iti.gov.br).

**Confidencialidade:** Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação (Disponível em: www.iti.gov.br).

**Criptografia**: Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito à formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem (Disponível em: www.iti.gov.br).

**Criptografia assimétrica ou de chaves públicas**: É um tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais (Disponível em: www.iti.gov.br).

**Criptografia simétrica ou de chave privada**: é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto. Para a garantia da integridade da informação transmitida é imprescindível que apenas o emissor e o receptor conheçam a chave. O problema da criptografia simétrica é a necessidade de compartilhar a chave secreta com todos que precisam ler a mensagem, possibilitando a alteração do documento por qualquer das partes (Disponível em: www.iti.gov.br).

**Infraestrutura de Chaves Públicas - ICP ou *Public Key Infrastrusture - PKI***: é um órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável. Sua principal função é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública.

**Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil**: É um conjunto de técnicas, arquitetura, organização, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Tem como objetivo estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em criptografia de chave pública, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A ICP-Brasil foi criada pela Medida Provisória 2200-2, de 24.08.2001 e está regulamentada pelas Resoluções do Comitê-Gestor da ICP-Brasil (Disponível em: www.iti.gov.br).

**Instituto Nacional de Tecnologia da Informação - ITI**: É uma autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil (Disponível em: www.iti.gov.br).

**Integridade**: Garantia oferecida ao usuário de que documento eletrônico, mensagem ou conjunto de dados não foi alterada, nem intencionalmente, nem acidentalmente por pessoas não autorizadas durantemitidos pela AC são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves. e sua transferência entre sistemas ou computadores.

**Não-repúdio**: ou não recusa, é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação.

**Sigilo**: Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas. Os titulares de certificados de assinatura digital

**Sistema**: é o conjunto de partes interagentes e interdependentes, que formam um todo unitário com determinado objetivo e que efetuam determinada função. Estes sistemas são compostos de subsistemas e supra sistemas, sendo fechados ou abertos, apresentando entropia positiva ou negativa (ALMEIDA, FREITAS e SOUZA (2011).

# APÊNDICES

**Apêndice A - Dimensões e temáticas para avaliação de impacto da Certificação Digital ICP-Brasil**

| DIMENSÕES | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ambiental A** | **Cultural C** | **Econômica E** | **Legal L** | **Política P** | **Social S** | **Tecnológica T** | **Territorial T** |
| Desmaterialização | Conscientização do cidadão | Agilidade nos processos | Assinatura Digital | Conflito de interesses | Acessibilidade | Atrativos acoplados à tecnologia | Aquisição de certificados de fora do país |
| Economia com transporte | Conscientização do governo | Comércio eletrônico | Autenticidade | Desburocratização | Cidadania | Biometria | Certificado do passaporte |
| | Conscientização do usuário profissional / organizacional | Custo do certificado | Cadeia de Confiança | Governança | Controle Social | Capacitação | Internacionalização |
| | Questão Cultural | Deslocamento do usuário para a emissão do CD | Carimbo do Tempo | ICP.com X ICP.gov / Tipo de Estrutura ICP | Elitização da certificação | Criptossistema | Migração de certificadoras de outros países |
| | Uso por terceiros | Economia com estrutura física | Confidencialidade | Interorganizações | Inclusão Digital | Desdobramentos da tecnologia | |
| | | Melhor aproveitamento de recursos | Fiscalização/ auditoria | Manutenção econômica da estrutura ICP | Massificação | Dificuldade de instalação | |
| | | Mercado | Fraudes | Modelo de negócio adotado | Transparência | Ferramenta amigável | |
| | | | Gestão documental | Modelo de processos | | Infraestrutura | |
| | | | Integridade | Novos projetos ITI | | Interoperabilidade | |
| | | | Lei de acesso | Origem da tecnologia com foco na defesa | | Logística de emissão/ reemissão do certificado | |
| | | | Não-repúdio | Rede de Capilaridade | | Novas aplicações da tecnologia | |
| | | | Segurança tecnológica x jurídica | | | Número de aplicações com utilização da tecnologia | |
| | | | Sigilo | | | Número de certificados emitidos | |
| | | | Validade jurídica | | | Pontos de venda | |
| | | | | | | Resistência ao uso | |
| | | | | | | Tecnologia imposta | |
| | | | | | | Tempo de emissão/ renovação do certificado | |

Fonte: o autor (2014).

**Apêndice B - Definição das temáticas**

| Dimensão | Temática | Definição da temática/Justificativa da temática na dimensão |
|---|---|---|
| Ambiental **A** | A-1. Desmaterialização. | Economia de papel. Economia com impressão de documentos e consumo de papel. A adoção da tecnologia acarreta a redução de impressão de documentos, que consequentemente, acarreta num menor desmatamento. |
| | A-2. Economia com transporte | Economia com transporte.A adoção da tecnologia permite a redução de transporte de documentos ou mesmo de pessoas, que anteriormente precisavam se deslocar para realizar atividades que antes não poderiam realizar remotamente por falta de segurança digital, o que impacta na redução de emissão de CO2. |
| Cultural **C** | C-1. Conscientização do cidadão | Cidadão passa a ter consciência da importância do uso da tecnologia. |
| | C-2 Conscientização do governo | Governo consciente da importância da adoção e uso da tecnologia. |
| | C-3. Conscientização do usuário profissional/ das organizações | Organizações e profissionais percebem a importância de uso da tecnologia para o desenvolvimento de suas atividades, importância da certificação nas carteiras de classe profissional, dentre outras questões e não mais apenas como uma obrigatoriedade. |
| | C-4. Questão Cultural | São os costumes. Resistência ao novo. Burocrática. Restritiva. |
| | C-5. Uso por terceiros | Mau uso.Uso indevido da tecnologia, uma vez que ela é uma tecnologia individual e intransferível, tendo estes dois fatores como premissa para existir. Neste caso, é considerado um uso consentido pelo proprietário da tecnologia. Seja porque não sabe utilizar ou por não querer utilizar. |
| Econômica **E** | E-1. Agilidade nos processos | Praticidade. A adoção da tecnologia permitiu uma maior agilidade nos processos das organizações, reduzindo tempo, fluxos, etc... tornando o processo mais prático, mais automatizado. |

| | | |
|---|---|---|
| | E-2. Comércio eletrônico | *E-commerce*.Comércio virtual. Compra e venda de mercadorias ou serviços por meio da internet |
| | E-3. Custo do certificado | Valor de mercado da tecnologia. Custo x Benefício. |
| | E-4. Deslocamento do usuário para a emissão do CD/ Identificação presencial | A emissão do certificado tem por exigência que o usuário vá até uma instalação técnica para realizar seu cadastro e posteriormente retorne para buscar o certificado, o que algumas vezes pode comprometer a adoção da tecnologia, seja pelo contratempo, seja porque em alguns locais não há instalação técnica na região. |
| | E-5. Economia com estrutura física | A tecnologia permite que os espaços físicos antes necessários para a guarda de grandes volumes de informações possam estar acessíveis de forma segura, integra e autêntica, não sejam mais necessários, pois as informações estão disponíveis remotamente. E ainda economia com espaços físicos para atendimento presencial. |
| | E-6. Melhor aproveitamento de recursos | O uso da tecnologia permite um melhor aproveitamento dos recursos da organização. |
| | E-7 Mercado | Certificação como negócio rentável / Oportunidade de negócio.Estrutura para emissão/venda da tecnologia é vista como um negócio rentável, como uma oportunidade de negócio. |
| Legal **L** | L-1. Assinatura Digital | Assinatura ou firma digital é um método de autenticação de informação digital, através de criptografia (o *hash* (resumo) e a encriptação deste *hash*). Ela providencia a prova inegável de que uma mensagem veio do emissor. Tem presente a autenticidade, integridade e irretratabilidade. |
| | L-2. Autenticidade | Garante que a informação é autêntica. |
| | L-3 Cadeia de Confiança | Também chamada de âncora de confiança, é a estrutura da ICP-Brasil, onde há uma cadeia de autoridades certificadoras, formada por uma Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (AC) e Autoridades de Registro (AR) e, |

| | | |
|---|---|---|
| | | ainda, por uma autoridade gestora de políticas, o Comitê Gestor da ICP-Brasil. Ou seja, cada autoridade certifica que a autoridade que está abaixo dela na hierarquia, possui todos os requisitos necessários para sua atuação |
| | L-4 Carimbo do tempo | Utilizado para garantir e assegurar a temporalidade de um documento digitalizado. |
| | L-5. Confidencialidade | É a garantia de que uma informação não será divulgada a indivíduos não autorizados. |
| | L-6. Fiscalização | Auditoria. Ato de verificação permanente das normas e especificações a atividades que envolvam a tecnologia, seja das certificadoras, seja das organizações que utilizam a tecnologia. |
| | L-7. Fraudes | Fraudes existem seja no meio físico, como no meio eletrônico. Já existem casos de tentativas de fraudes com certificação digital. Utilização indevida da tecnologia. |
| | L-8 Gestão documental | Ciclo de vida do documento digital. O uso da tecnologia altera os procedimentos de gestão documental, por estar em outra plataforma e exige que se pense em como tratar o que fica para trás, o documento em papel, ou demais mídias materiais. |
| | L-9. Integridade | Garante que uma informação não foi modificada. |
| | L-10. Lei de Acesso | A Lei nº 12.527/2011 regulamenta o direito constitucional de acesso às informações públicas. Criou mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.A Lei vale para os três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Conta e Ministério Público. |
| | L-11. Não-repúdio | Impossibilidade de negar uma ação (não recusa). Usuário como único responsável pelas transações realizadas com o uso da tecnologia. |
| | L-12. Segurança tecnológica x jurídica | Tecnologia como ferramenta de segurança, seja segurança tecnológica ou jurídica. |

| | | |
|---|---|---|
| | L-13 Sigilo | Privacidade. É uma informação ou conhecimento que pode resultar em uma perda de vantagem ou do nível de segurança, caso revelada a terceiros, que podem resultar em baixa ou desconhecida confiabilidade ou intenção. A perda, o mau uso, a modificação ou o acesso não autorizado pode afetar a privacidade ou bem-estar de um indivíduo, organização ou até mesmo a segurança de um país. |
| | L-14. Validade jurídica | Garantia Jurídica. Garante que as transações eletrônicas tenham o mesmo valor legal. |
| Política **P** | P-1. Conflito de interesses | Questões políticas.Os interesses, seja de governamental ou privado, são diferentes e podem impactar a difusão e na adoção da tecnologia. |
| | P-2. Desburocratização | Tecnologia permitiu simplificar processos e normas e trâmites. |
| | P-3. Governança | É o conjunto de práticas, padrões, processos, regulamentos, decisões, costumes, ideias por onde se quer seguir. Estado de direito, transparência, responsabilidade, orientação por consenso, igualdade e inclusão, efetividade e eficiência e prestação de contas. |
| | P-4. ICP.com X ICP.gov | Tipo de estrutura ICP. A origem da Infraestrutura de Chaves Públicas Brasileira era governamental, mas acabou tomando um rumo comercial. Ambas não focaram inicialmente o cidadão. Tipo da estrutura de chaves públicas adotada (Composta por uma AC-Raiz, AC's e AR's.) |
| | P-5. Interorganizações | Parcerias / convênios.Representa as relações entre organizações que fortalecem a tecnologia e consequentemente refletem na sua disseminação. |
| | P-6. Manutenção econômica da estrutura ICP | Não há um retorno direto de lucratividade para o governo, há uma preocupação de como manter economicamente uma estrutura onerosa como esta. |
| | P-7. Modelo de negócio adotado | Foco da estrutura ICP.Algumas autoridades certificadoras veem na tecnologia uma forma de negócio e agilizam a sua disponibilização ao usuário, outras não. Umas |

| | | |
|---|---|---|
| | | mais burocráticas apesar da padronização de exigências. |
| | P-8. Modelo de processo | Tecnologia altera os modelos de processos na organização. |
| | P-9. Novos projetos ITI | Carro chefe.Representa os novos projetos a serem lançados pelo ITI e seu projeto principal projeto mais importante para a disseminação da tecnologia. |
| | P-10. Origem da tecnologia com foco na defesa | A origem da tecnologia se deu por questões de defesa do país. |
| | P.11. Rede de Capilaridade | Capaz de produzir uma rede de fenômenos ligados a tecnologia. Fluidez. |
| Social **S** | S-1. Acessibilidade | Ampliação de acesso às informações.A tecnologia permitiu um aumento no acesso a informações. |
| | S-2. Cidadania | É o exercício dos direitos e deveres civis, políticos e sociais estabelecidos na constituição, onde direitos e deveres estão interligados. |
| | S-3. Controle Social | E-social.Sociedade acompanha as ações do governo. |
| | S-4. Elitização da certificação | CD corporativa.Somente alguns grupos têm acesso e obrigatoriedade de uso, seja pela área de atuação, seja pelo custo. |
| | S-5. Inclusão Digital | Tecnologia permite a inclusão digital, que é o nome dado ao processo de democratização do acesso às TIC's, permitindo a inserção de todos na sociedade da informação, onde estão inclusos os instrumentos básicos: dispositivo para conexão, acesso à rede e o domínio das ferramentas computacionais. |
| | S.6 Massificação | Disseminação do uso/ Política de disseminação da tecnologia.Tecnologia para ser adotada em grande escala, necessita de divulgação, difusão. |

| | | |
|---|---|---|
| | S-7. Transparência | Tecnologia permite uma maior transparência dos órgãos públicos e empresas privadas. É o amplo acesso e divulgação das informações. |
| Tecnológica **T** | T-1. Atrativos acoplados à tecnologia | A tecnologia necessita da inserção de itens que chamem a atenção do usuário/cliente, que podem não contribuir em nada com seu objetivo final, apenas para atrair para sua adoção. |
| | T-2. Biometria | Pode ser impressão digital, reconhecimento facial, reconhecimento da Iris ou de retina, dentre outras. É um dos métodos mais seguros de identificação, uma vez que faz uso de técnicas de reconhecimento de características únicas de cada pessoa. É uma medição biológica das características físicas e comportamentais de cada pessoa. |
| | T-3 Capacitação | Treinamento. Consultoria. Tecnologia necessita capacitação para sua utilização. |
| | T-4. Criptossistema | É definido[6] como o quíntuplo (m, C, K, E e D), onde:m representa o conjunto de todas as mensagens não criptografadas (texto simples) que podem ser enviados.C representa o conjunto de todas as cifras possíveis ou mensagens criptogramas.K representa o conjunto de chaves que podem ser usados em sistema de criptografia.E é o conjunto de transformações de criptografia ou família de funções aplicada a cada elemento de m para se obter um elemento de C . Há uma transformação diferente E k para cada possível valor de chave K. E D é o conjunto de transformações descriptografia análogas E |
| | T-5. Desdobramentos da tecnologia | Duplica-se certificado, para que um terceiro possa realizar atividades e um último usuário valide. |
| | T-6. Dificuldade de instalação | A tecnologia não é de fácil instalação. É necessária configuração. Muitos passos para configuração. Muitas vezes necessita suporte técnico. |

[6] Fonte: http://www.segu-info.com.ar/criptologia/criptosistema.htm

| | | |
|---|---|---|
| | T-7 Ferramenta amigável | Facilidade de uso / Usabilidade.Tecnologia de fácil utilização, ferramenta amigável. |
| | T-8. Infraestrutura | Estrutura de software, hardware, instalações técnicas, energia elétrica, etc. estrutura mínima necessária para atingir à todos os cidadãos no país. |
| | T-9. Interoperabilidade | Unificação/ integração/ adequação/ Compatibilidade de sistemas/bases.Os sistemas não são integrados ou compatíveis, necessitam adequação, unificação. |
| | T-10. Logística de emissão/reemissão de certificado | Processo de emissão/reemissão. É burocrático, às vezes demorado (tempo médio de emissão varia de acordo com a AC, de meses a minutos) e presencial. Autoridades Certificadoras precisam estar preparadas para emissões e renovações de certificados em larga escala, para que o processo não se torne demorado e faça com que perca usuários. |
| | T-11 Novas aplicações da tecnologia | Serviço estruturante. Está relacionado aos novos projetos, onde novos aplicativos são desenvolvidos e disponibilizados. |
| | T-12. Número de aplicações com utilização da tecnologia | Número de aplicações que permitem a utilização da tecnologia é reduzido. |
| | T-13. Número de emissões | Número de certificados emitidos reflete o impacto desta tecnologia. Pode ser visto como positivo ou negativo dependendo da visão do entrevistado, em relação ao período de existência da tecnologia. |
| | T-14. Ponto de venda | Instalações técnicas.Número de pontos de venda, instalações técnicas de emissão e renovação da tecnologia. |
| | T-15. Resistência ao uso | Diversos profissionais em todas as esferas têm/tiveram resistência ao uso da tecnologia, tentando postergar sua aquisição e até mesmo concedendo a terceiros o seu próprio certificado, que é único e intransferível. |
| | T-16. Tecnologia imposta | Obrigatoriedade do uso da tecnologia por parte do governo. |

| | | |
|---|---|---|
| | T-17. Tempo de emissão/ renovação do certificado | A tecnologia possui prazo de validade específico, necessitando renovação a cada 3 ou 5 anos, dependendo do seu tipo. A reemissão de novo certificado não é instantânea. |
| Territorial **T** | TR-1. Aquisição de certificados de fora do país | As possíveis falhas fragilidades da certificação ICP-Brasil podem fazer com que se busquem certificados fora do país. |
| | TR-2 Certificação do passaporte | Passaporte com uso de certificado digital. |
| | TR-3. Internacionalização | Aceitabilidade em outros países.Possibilidade de o certificado digital brasileiro ser aceito em outros países, através de acordos e fiscalização internacional. |
| | TR-4. Migração de certificadoras de outros países | Uma vez que no Brasil está tecnologia ainda está em processo de disseminação e tem um alto custo para o usuário, certificadoras consagradas em outros países podem ver este ramo como um bom investimento e migrar para o Brasil criando novas regras. |

Fonte: o autor.

**Apêndice C –Termo de Consentimento Livre e Esclarecido – TCLE**
**Roteiro das entrevistas**

Gostaríamos de lhe convidar a participar da pesquisa "**Avaliação de Impacto Socioeconômico da Certificação Digital no Brasil**", sob a coordenação da pesquisadora Gertrudes Aparecida Dandolini. Essa pesquisa decorre do Termo de Cooperação Nº 02/2012 do Instituto Nacional de Tecnologia da Informação – ITI, Autarquia Federal vinculada à Casa Civil da Presidência da República e órgão gestor da Certificação Digital no Brasil, firmado com a Universidade Federal de Santa Catarina – UFSC, por meio do Núcleo de Estudos em Inovação, Gestão e Tecnologia da Informação (IGTI/UFSC).

Essa pesquisa compreende a execução de uma Avaliação de Impacto Socioeconômico – AISE da Certificação Digital – CD no Brasil, e para tanto, iremos: a) realizar um mapeamento da situação atual da CD no Brasil; b) identificar e definir as dimensões de mensuração do impacto socioeconômico; c) propor um modelo de análise de impacto; e por fim, d) identificar potencialidades e adversidades da CD no Brasil.

A execução da AISE será feita por meio de quatro módulos, sendo: 1 – definição do escopo da AISE; 2 – delineamento do *survey;* 3 – coleta e análise dos dados; e 4 – interpretação dos dados e resultados. Assim, de forma a alcançar os objetivos, serão realizadas entrevistas semiestruturadas sobre o tema Certificação Digital. Dado o caráter exploratório dessa fase da pesquisa, vossa participação pode ser requerida em um segundo momento, caso a análise das entrevistas indiquem pontos específicos que necessitam de aprofundamento.

Esclarecemos que:

2 a participação é totalmente voluntária, podendo recusar-se, ou mesmo retirar vossa permissão a qualquer momento. As informações prestadas serão utilizadas somente para os fins desta pesquisa e serão tratadas com o mais absoluto sigilo e de modo a preservar a identidade pessoal e da instituição;

3 durante a análise dos dados, tanto os registros sonoros das entrevistas quanto os textos resultantes das transcrições serão arquivados e apenas os pesquisadores envolvidos com o projeto terão acesso aos dados. Qualquer característica, nome, estratégia de negócio ou evento que possibilite a identificação dos entrevistados e de suas instituições serão omitidas, a fim de manter o direito constitucional a privacidade; e

4 durante todo o período da pesquisa fica reservado o direito de sanar qualquer dúvida ou solicitar qualquer outro esclarecimento, bastando para isso entrar em contato, com algum dos pesquisadores.

Caso hajam dúvidas ou necessidade de outros esclarecimentos, pode ser realizado contato com os Professores Drª Gertrudes Aparecida Dandolini ou Dr. João Artur de Souza - telefone (48) 3721 4044 ou e-mail gtude@egc.ufsc.br / jartur@egc.ufsc.br.

Este termo deverá ser preenchido em duas vias de igual teor.
Autorização:

Eu,
_____,
após a leitura deste documento e sanadas as dúvidas quanto à minha participação, acredito estar suficientemente informado quanto à pesquisa e seus procedimentos, ficando claro que minha participação é voluntária e que posso retirar este consentimento a qualquer momento. Diante do exposto expresso minha concordância de espontânea vontade em participar desta pesquisa.

Local: _____

Data: _____

_____
Assinatura do Participante

Declaramos que obtivemos de forma apropriada e voluntária o Consentimento Livre e Esclarecido.

_____
João Artur de Souza
Pesquisador responsável - IGTI

_____
Ruy César Ramos Filho
Assessor Técnico ITI - Representante ITI

_____
Maria Isabel Araújo Silva dos Santos
Pesquisadora IGTI

**Apêndice D – Roteiro das entrevistas**

Comente sobre a percepção dos itens abaixo no aspecto importância no passado (antes da CD) no presente como fatores de importância para a tomada de decisões da empresa (ou do setor da empresa), e quais são necessárias para a projeção de cenários futuros otimistas e pessimistas?

| | |
|---|---|
| **CONTEXTUALIZAÇÃO** | – Como utiliza a CD? (Contexto geral e específico)<br>– Impactos percebidos na Implantação<br>– Impactos percebidos na Utilização<br>– Novo contexto da CD (cenário atual X cenário anterior)<br>– Resistência na implantação (processo de capacitação, treinamento, sensibilização, interno, externo, ...)<br>– Quais pontos positivos e negativos com a utilização?<br>– Administração sem papel? (É uma realidade?)<br>– **Riscos** relativos a Certificação Digital? (Cenário pessimista) |
| **Tecnológico** | – **Novas tecnologias** surgiram a partir da implementação da CD? Quais?<br>– Tecnologias alternativas à CD? (Segundo plano – *login* e senha)<br>– Infraestrutura para adoção e uso da CD?<br>– Padrões nos equipamentos?<br>– Certificado de atributos?<br>– Ferramenta amigável? |
| **Política** | – Melhoria do relacionamento entre instituições?<br>– Melhoria no relacionamento com o cidadão?<br>– Governo eletrônico? |
| **Econômica** | – Facilitação da produção de bens e serviços?<br>– Aumento da arrecadação de tributos?<br>– Melhoria nos modelos de negócio?<br>– Aumento do consumo de bens e serviços?<br>– Maturidade nos serviços?<br>– Permite um reaproveitamento de recursos? |

| | |
|---|---|
| **Social** | – Melhoria de acesso à informação?<br>– Melhoria da Transparência?<br>– Relação com o cidadão / consumidor?<br>– Emprego – benefício?<br>– Melhoria na condição de vida?<br>– Acessibilidade a CD? (Exclusão x Inclusão) |
| **Cultural** | – Resistência ao uso?<br>– Conscientização? |
| **Ambiental** | – Existem economias com relação a recursos naturais?<br>– Desmaterialização dos processos? |
| **Legal** | – Integridade, confiabilidade, segurança, portabilidade, autenticidade, não repúdio?<br>– Aumento da segurança de transação de informações? |
| **Territorial** | – ICP e certificação em outros países? |

Fonte: IGTI (2013)